IBM

Integriertes Managementmodul I
Benutzerhandbuch

Integriertes Managementmodul I
Benutzerhandbuch

Siebte Ausgabe (Dezember 2013)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Integrated Management Module I, User's Guide,
IBM Teilenummer 00FH192,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
Dezember 2013

Inhaltsverzeichnis

Tabellen

Kapitel 1. Einführung

Das integrierte Managementmodul (IMM) konsolidiert die Serviceprozessorfunktionalität, Super-E/A-Funktionen, Videocontrollerfunktionen und eine Remote-Presence-Funktion in einem einzigen Chip auf der Serversystemplatine. Das IMM ersetzt damit den Baseboard Management Controller (BMC) und den Remote Supervisor Adapter II in IBM® System x Servern.

Bevor das IMM in IBM Servern verwendet wurde, waren der Baseboard Management Controller (BMC) und das Basic Input/Output System (BIOS) die Standardhardware und -firmware für das Systemmanagement. System x Server verwendeten BMC-Serviceprozessoren zum Verwalten der Schnittstelle zwischen Systemmanagementsoftware und Plattformhardware. Der Remote Supervisor Adapter II und der Remote Supervisor Adapter II Slimline waren Zusatzeinrichtungen, die als Controller für Außerband-Server-Management fungierten.

Wichtig: Obwohl das IMM in einigen IBM BladeCenter-Produkten und IBM Blade-Servern standardmäßig enthalten ist, bleibt das erweiterte BladeCenter-Managementmodul das primäre Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für BladeCenter und Blade-Server. Die Inhalte, die in Beziehung zur IMM-Webschnittstelle und zur Befehlszeilenschnittstelle stehen, sind für IBM BladeCenter und Blade-Server nicht anwendbar. Benutzer, die die IMM-Einstellungen auf Blade-Servern konfigurieren möchten, sollten dazu das Dienstprogramm für erweiterte Einstellungen auf dem Blade-Server verwenden.

Das IMM bietet einige Verbesserungen im Vergleich zur kombinierten Funktionalität des BMC und des Remote Supervisor Adapters II:

- Die Auswahl einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung. Die dedizierte Ethernet-Verbindung ist auf Blade-Servern und auf einigen System x Servern nicht verfügbar.

  Anmerkung: Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze. Wenn auf Ihrer Hardware kein Anschluss für dedizierte Netze vorhanden ist, ist die Einstellung *shared* (gemeinsam genutzt) die einzig verfügbare IMM-Einstellung.
- Eine gemeinsame IP-Adresse für IPMI (Intelligent Platform Management Interface) und die Serviceprozessorschnittstelle. Diese Funktion ist für Blade-Server nicht verfügbar.
- Embedded Dynamic System Analysis (DSA).
- Die Möglichkeit, lokale oder ferne Aktualisierungen anderer Einheiten durchzuführen, ohne dass ein Neustart des Servers zum Initialisieren des Aktualisierungsprozesses erforderlich ist.
- Ferne Konfiguration mit dem Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU). Diese Funktion ist für Blade-Server nicht verfügbar.
- Die Möglichkeit für Anwendungen und Tools, zwischen Außerband- oder Inbandzugriff auf das IMM zu wählen. Auf Blade-Servern werden nur Inbandverbindungen zum IMM unterstützt.
- Erweiterte Remote Presence-Funktionalität. Diese Funktion ist für Blade-Server nicht verfügbar.

Die IBM System x® Server-Firmware ist die IBM Implementierung der UEFI (Unified Extensible Firmware Interface). Sie ersetzt das BIOS in System x Servern und IBM Blade-Servern. Das BIOS war der Standardfirmwarecode, der die grundlegenden Hardwareoperationen, wie z. B. Interaktionen mit Diskettenlaufwerken, Festplattenlaufwerken und der Tastatur, steuerte. Die IBM System x Server-Firmware bietet mehrere zusätzliche Funktionen, die im BIOS nicht zur Verfügung stehen, einschließlich Kompatibilität mit UEFI 2.1, iSCSI-Kompatibilität, Active Energy Manager-Technologie und erweiterte Zuverlässigkeits- und Servicekompetenz. Das Konfigurationsdienstprogramm bietet Serverinformationen, Serverkonfiguration und Anpassungskompatibilität sowie die Möglichkeit, die Bootreihenfolge festzulegen.

Anmerkungen:

- In diesem Dokument wird die IBM System x Server-Firmware oft als "Server-Firmware" und gelegentlich als "UEFI" bezeichnet.
- Die IBM System x Server-Firmware ist vollständig kompatibel mit Betriebssystemen ohne UEFI.
- Weitere Informationen zur Verwendung der IBM System x Server-Firmware finden Sie in der Dokumentation, die mit Ihrem Server geliefert wurde.

In diesem Dokument wird erläutert, wie die Funktionen des IMM in einem IBM Server verwendet werden. Das IMM stellt mithilfe der IBM System x Server-Firmware Systemverwaltungsfunktionen für System x- und BladeCenter-Server bereit.

Dieses Dokument enthält keine Erklärungen von Fehlern oder Nachrichten. Eine Beschreibung der IMM-Fehler und -Nachrichten finden Sie im Fehlerbestimmungs- und Servicehandbuch für Ihren Server. Gehen Sie wie im Folgenden beschrieben vor, um die aktuellste Version diese Dokuments oder des IBM White Paper *Transitioning to UEFI and IMM* (Statusänderung zu UEFI und IMM) im IBM® Support Portal zu suchen.

Anmerkung: Beim ersten Zugriff auf das IBM Support Portal müssen Sie die Produktkategorie, die Produktfamilie und die Modellnummern Ihres Server auswählen. Wenn Sie das nächste Mal auf das IBM Support Portal zugreifen, werden die Produkte, die Sie beim ersten Mal ausgewählt haben, von der Website erneut geladen, sodass nur die Links für Ihre Produkte angezeigt werden. Um Ihre Produktliste zu ändern oder Elemente zu ihr hinzuzufügen, klicken Sie auf den Link **Manage my product lists** (Meine Produktlisten verwalten).

Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die Vorgehensweisen zum Bestimmen der Firmware und der Dokumentation weicht möglicherweise geringfügig von den Beschreibungen im vorliegenden Dokument ab.

1. Wechseln Sie zu http://www.ibm.com/support/entry/portal.
2. Wählen Sie unter **Choose your products** (Produkt auswählen) die Option **Browse for a product** (Nach Produkt suchen) aus und erweitern Sie **Hardware**.
3. Klicken Sie je nach Servertyp auf **Systems** > **System x** oder **Systems** > **BladeCenter** und wählen Sie die Felder für Ihre Server aus.
4. Klicken Sie unter **Choose your task** (Task auswählen) auf **Documentation**.
5. Klicken Sie unter **See your results** (Ergebnisse anzeigen) auf **View your page** (Ihre Seite anzeigen).
6. Klicken Sie im Feld "Documentation" auf **More results** (Weitere Ergebnisse).

7. Wählen Sie im Feld "Category" das Kontrollkästchen **Integrated Management Module (IMM)** aus. Die Links zur Dokumentation zum IMM und zur UEFI werden angezeigt.

Wenn Firmwareaktualisierungen verfügbar sind, können Sie sie von der IBM Website herunterladen. Das IMM verfügt möglicherweise über Produktmerkmale und Funktionen, die in der Dokumentation nicht beschrieben sind. Möglicherweise wird die Dokumentation gelegentlich mit Informationen zu diesen Produktmerkmalen und Funktionen aktualisiert oder es werden technische Aktualisierungen mit weiteren Informationen, die nicht in der Dokumentation zum IMM enthalten sind, bereitgestellt.

Gehen Sie wie folgt vor, um zu prüfen, ob Firmwareaktualisierungen verfügbar sind.

Anmerkung: Beim ersten Zugriff auf das IBM Support Portal müssen Sie die Produktkategorie, die Produktfamilie und die Modellnummern Ihres Server auswählen. Wenn Sie das nächste Mal auf das IBM Support Portal zugreifen, werden die Produkte, die Sie beim ersten Mal ausgewählt haben, von der Website erneut geladen, sodass nur die Links für Ihre Produkte angezeigt werden. Um Ihre Produktliste zu ändern oder Elemente zu ihr hinzuzufügen, klicken Sie auf den Link **Manage my product lists** (Meine Produktlisten verwalten).

Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die Vorgehensweisen zum Bestimmen der Firmware und der Dokumentation weicht möglicherweise geringfügig von den Beschreibungen im vorliegenden Dokument ab.

1. Wechseln Sie zu http://www.ibm.com/support/entry/portal.
2. Wählen Sie unter **Choose your products** (Produkt auswählen) die Option **Browse for a product** (Nach Produkt suchen) aus und erweitern Sie **Hardware**.
3. Klicken Sie je nach Servertyp auf **Systems** > **System x** oder **Systems** > **BladeCenter** und wählen Sie die Felder für Ihre Server aus.
4. Klicken Sie unter **Choose your task** (Task auswählen) auf **Downloads**.
5. Klicken Sie unter **See your results** (Ergebnisse anzeigen) auf **View your page** (Ihre Seite anzeigen).
6. Klicken Sie im Feld "Flashes & Alerts" auf den Link für den betreffenden Download oder klicken Sie auf **More results**, um weitere Links anzuzeigen.

IMM-Produktmerkmale

Das IMM stellt die folgenden Funktionen bereit:

- Fernzugriff und Fernverwaltung Ihres Servers rund um die Uhr
- Fernverwaltung unabhängig vom Status des verwalteten Servers
- Fernsteuerung der Hardware und der Betriebssysteme
- Webbasierte Verwaltung mithilfe von Standard-Web-Browsern

IMM stellt zwei Arten von IMM-Funktionalität bereit: IMM Standard-Produktmerkmale und IMM Premium-Produktmerkmale. Informationen dazu, welche Art von IMM-Hardware in Ihrem Server installiert ist, finden Sie in der Dokumentation im Lieferumfang Ihres Servers.

IMM Standard-Produktmerkmale

Anmerkung: Einige der folgenden Produktmerkmale sind für Blade-Server nicht verfügbar.

- Zugriff auf kritische Servereinstellungen
- Zugriff auf elementare Produktdaten (VPD)
- Erweiterte Unterstützung für PFA (Predictive Failure Analysis)
- Automatische Benachrichtigungen und Alerts
- Ständige Überwachung und Steuerung des ordnungsgemäßen Betriebs
- Auswahl einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung (falls anwendbar).

  Anmerkung: Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze.
- Unterstützung für DNS-Server (Domain Name System)
- DHCP-Unterstützung (Dynamic Host Configuration Protocol)
- E-Mail-Alerts
- Integrierte DSA (Dynamic System Analysis)
- Erweiterte Benutzerberechtigungsstufen
- LAN over USB für Inbandkommunikation zum IMM
- Ereignisprotokolle mit Zeitmarken, die auf dem IMM gespeichert werden und an E-Mail-Alerts angehängt werden können
- Dem Branchenstandard entsprechende Schnittstellen und Protokolle
- Betriebssystem-Watchdogs
- Ferne Konfiguration über das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU).
- Ferne Firmwareaktualisierungen
- Ferne Steuerung der Stromversorgung
- Nahtlose Remoteunterstützung für erweiterte Grafikfunktionen
- Benutzerschnittstelle für sicheren Web-Server
- Serial over LAN
- Serverkonsolenumleitung
- Unterstützung für SNMP (Simple Network Management Protocol)
- Benutzerauthentifizierung mithilfe einer sicheren Verbindung zu einem LDAP-Server (Lightweight Directory Access Protocol)

IMM Premium-Produktmerkmale

Anmerkung: Einige der folgenden Produktmerkmale sind für Blade-Server nicht verfügbar.

- Zugriff auf kritische Servereinstellungen
- Zugriff auf elementare Produktdaten (VPD)
- Erweiterte Unterstützung für PFA (Predictive Failure Analysis)
- Automatische Benachrichtigungen und Alerts
- Ständige Überwachung und Steuerung des ordnungsgemäßen Betriebs
- Auswahl einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung (falls anwendbar).

  Anmerkung: Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze.
- Unterstützung für DNS-Server (Domain Name System)
- DHCP-Unterstützung (Dynamic Host Configuration Protocol)
- E-Mail-Alerts
- Integrierte DSA (Dynamic System Analysis)
- Erweiterte Benutzerberechtigungsstufen
- LAN over USB für Inbandkommunikation zum IMM
- Ereignisprotokolle mit Zeitmarken, die auf dem IMM gespeichert werden und an E-Mail-Alerts angehängt werden können
- Dem Branchenstandard entsprechende Schnittstellen und Protokolle
- Betriebssystem-Watchdogs
- Ferne Konfiguration über das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU).
- Ferne Firmwareaktualisierungen
- Ferne Steuerung der Stromversorgung
- Nahtlose Remoteunterstützung für erweiterte Grafikfunktionen
- Benutzerschnittstelle für sicheren Web-Server
- Serial over LAN
- Serverkonsolenumleitung
- Unterstützung für SNMP (Simple Network Management Protocol)
- Benutzerauthentifizierung mithilfe einer sicheren Verbindung zu einem LDAP-Server (Lightweight Directory Access Protocol)
- Remote Presence-Funktion, einschließlich der Fernsteuerung eines Servers
- Anzeigenerfassung von Betriebssystemfehlern und Anzeige über die Webschnittstelle
- Ferne Datenträger; die ermöglicht den Anschluss eines Diskettenlaufwerks, CD-/DVD-Laufwerks, USB-Flashlaufwerks oder eines Plattenimage an den Server

Anmerkung: Die folgenden Produktmerkmale des Remote Supervisor Adapter II werden nicht vom IMM bereitgestellt:

- Anzeige von Server-MAC-Adressen
- Mehrfache NTP-Servereinträge

Upgrade von IMM Standard auf IMM Premium durchführen

Wenn Ihr Server über die IMM Standard-Funktionalität verfügt, können Sie ein Upgrade auf IMM Premium durchführen, indem Sie einen Virtual Media Key erwerben und ihn auf der Serversystemplatine installieren. Es ist keine neue Firmware erforderlich.

Rufen Sie die Website http://www.ibm.com/systems/x/newgeneration auf, um einen Virtual Media Key zu bestellen.

Anmerkung: Informationen zur Installation des Virtual Media Key finden Sie in der Dokumentation, die mit Ihrem Server geliefert wurde.

Wenn Sie Hilfe bei Ihrer Bestellung benötigen, rufen Sie die gebührenfreie Telefonnummer an, die auf der Seite mit den Einzelhandelsteilen aufgeführt ist, oder wenden Sie sich an den zuständigen IBM Ansprechpartner vor Ort, um Unterstützung zu erhalten.

Vergleich des IMM mit anderer Systemmanagement-Hardware in System x Servern

In der folgenden Tabelle werden die IMM-Produktmerkmale mit den Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern verglichen.

Anmerkung: Wie der BMC verwendet auch das IMM die IPMI-Standardspezifikation.

Tabelle 1. Vergleich der IMM-Produktmerkmale mit den kombinierten Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern

Beschreibung	BMC mit Remote Supervisor Adapter II	IMM
Netzverbindungen	Der BMC verwendet eine Netzverbindung gemeinsam mit einem Server und einer IP-Adresse, die sich von der IP-Adresse des Remote Supervisor Adapter II unterscheidet. Der Remote Supervisor Adapter II verwendet eine dedizierte Systemmanagementnetzverbindung und eine IP-Adresse, die sich von der IP-Adresse des BMC unterscheidet.	Das IMM stellt sowohl die Funktionalität des BMC als auch die des Remote Supervisor Adapter II über dieselbe Netzverbindung bereit. Dabei wird nur eine IP-Adresse verwendet. Wenn Ihr Server über einen dedizierten Netzanschluss für das Systemmanagement verfügt, können Sie zwischen einer dedizierten oder einer gemeinsam genutzten Netzverbindung wählen. **Anmerkung:** Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze. Wenn auf Ihrer Hardware kein Anschluss für dedizierte Netze vorhanden ist, ist die Einstellung *Shared* (Gemeinsam genutzt) die einzig verfügbare IMM-Einstellung.
Aktualisierungs-funktionalität	Für jeden Server ist eine eindeutige Aktualisierung für den BMC und den Remote Supervisor Adapter II erforderlich. Das BIOS und die Diagnosetools können mit einem Inbandverfahren aktualisiert werden.	Ein IMM-Firmware-Image kann für alle maßgeblichen Server verwendet werden. Die IMM-Firmware, die Server-Firmware für System x und die Dynamic System Analysis-Firmware (DSA) können sowohl im Außerband- als auch im Inbandverfahren aktualisiert werden. Das IMM kann sich selbst, die Server-Firmware und die Dynamic System Analysis-Firmware lokal oder über Fernzugriff aktualisieren, ohne dass der Server erneut gestartet werden muss, um den Aktualisierungsprozess zu initialisieren.

Tabelle 1. Vergleich der IMM-Produktmerkmale mit den kombinierten Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern (Forts.)

Beschreibung	BMC mit Remote Supervisor Adapter II	IMM
Konfigurations-funktionalität	Konfigurationsänderungen mit dem Dienstprogramm für erweiterte Einstellungen (ASU) sind nur im Inbandverfahren verfügbar. Für das System sind separate Konfigurationen für den BMC, den Remote Supervisor Adapter II und das BIOS erforderlich.	Das Dienstprogramm für erweiterte Einstellungen kann im Inband- und im Außerbandverfahren ausgeführt werden. Es kann sowohl das IMM als auch die Server-Firmware konfigurieren. Mit dem Dienstprogramm für erweiterte Einstellungen können Sie außerdem die Bootreihenfolge, die iSCSI und die elementaren Produktdaten (VPD) (Maschinentyp, Seriennummer, UUID und Asset ID) ändern. Die Konfigurationseinstellungen der Server-Firmware werden über das IMM gespeichert und verwaltet. Aus diesem Grund können Sie Konfigurationsänderungen an der Server-Firmware vornehmen, während der Server ausgeschaltet ist oder während das Betriebssystem ausgeführt wird. Diese Änderungen werden wirksam, wenn der Server das nächste Mal gestartet wird. Die IMM-Konfigurationseinstellungen können im Inband- und im Außerbandverfahren über die folgenden IMM-Benutzerschnittstellen konfiguriert werden: • Webschnittstelle • Befehlszeilenschnittstelle • IBM Systems Director-Schnittstelle • SNMP
Erfassung der Betriebssystem- anzeige	Anzeigenerfassungen werden beim Auftreten von Betriebssystemfehlern vom Remote Supervisor Adapter II erstellt. Für die Anzeige von Anzeigenerfassungen ist ein Java-Applet erforderlich.	Diese Funktion ist nur mit IMM Premium verfügbar. Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade von IMM Standard auf IMM Premium durchführen" auf Seite 6. Anzeigenerfassungen werden direkt im Web-Browser angezeigt. Ein Java-Applet ist nicht erforderlich.

Tabelle 1. Vergleich der IMM-Produktmerkmale mit den kombinierten Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern (Forts.)

Beschreibung	BMC mit Remote Supervisor Adapter II	IMM
Fehlerprotokollierung	Der BMC stellt ein BMC-Systemereignisprotokoll (IPMI-Ereignisprotokoll) bereit. Der Remote Supervisor Adapter II stellt ein textbasiertes Protokoll bereit, das Beschreibungen der Ereignisse umfasst, die vom BMC gemeldet werden. Dieses Protokoll enthält außerdem alle Informationen oder Ereignisse, die vom Remote Supervisor Adapter II selbst festgestellt wurden.	Das IMM verfügt über zwei Ereignisprotokolle: 1. Das Systemereignisprotokoll ist über die IPMI-Schnittstelle verfügbar. 2. Das Gehäuseereignisprotokoll ist über die anderen IMM-Schnittstellen verfügbar. Im Gehäuseereignisprotokoll werden Textnachrichten angezeigt, die mithilfe der Spezifikationen DSP0244 und DSP8007 für die Distributed Management Task Force generiert wurden. **Anmerkung:** Erklärungen zu den einzelnen Ereignissen und Nachrichten finden Sie im Fehlerbestimmungs- und Servicehandbuch zu Ihrem Server.
Überwachung	Der BMC mit dem Remote Supervisor Adapter II verfügt über die folgenden Überwachungsfunktionen: • Überwachung der Server- und Batteriespannung, Servertemperatur, Lüfter, Netzteile sowie des Prozessor- und DIMM-Status • Steuerung der Lüftergeschwindigkeit • Unterstützung für PFA (Predictive Failure Analysis) • Steuerung der Systemdiagnoseanzeigen (Stromversorgung, Festplattenlaufwerk, Aktivität, Alerts und Überwachungssignal) • Automatischer Neustart des Servers (ASR - Automatic Server Restart) • Automatische Wiederherstellung des BIOS (ABR - Automatic BIOS Recovery)	Das IMM stellt dieselben Überwachungsfunktionen wie der BMC und der Remote Supervisor Adapter II bereit. In RAID-Konfiguration unterstützt das IMM außerdem einen erweiterten Festplattenlaufwerkstatus, einschließlich einer Plattenlaufwerk-PFA.

Tabelle 1. Vergleich der IMM-Produktmerkmale mit den kombinierten Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern (Forts.)

Beschreibung	BMC mit Remote Supervisor Adapter II	IMM
Remote Presence	Der BMC mit dem Remote Supervisor Adapter II verfügt über die folgenden Remote-Presence-Funktionen: • Umleitung an die Grafikkonsole über LAN • Fernes virtuelles Disketten- und CD-ROM-Laufwerk • Ferne Hochgeschwindigkeitsumleitung von PCI-Bildschirm, -Tastatur und -Maus • Unterstützte Bildschirmauflösung bis zu 1024 x 768 mit 70 Hz • Datenverschlüsselung	Diese Funktion ist nur mit IMM Premium verfügbar. Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade von IMM Standard auf IMM Premium durchführen" auf Seite 6. Zusätzlich zu den Remote-Presence-Funktionen des Remote Supervisor Adapter II bietet das IMM folgende Funktionalität. **Anmerkung:** Für das IMM ist das Java Runtime Environment ab Version 1.5 oder ActiveX erforderlich, wenn der Internet Explorer unter Windows verwendet wird. • Unterstützte Bildschirmauflösung bis zu 1280 x 1024 mit 75 Hz • USB-2.0-Unterstützung für virtuelle Tastatur, Maus und Massenspeichereinheiten • 15-Bit-Farbtiefe • Auswahl eines absoluten oder relativen Mausmodus • Unterstützung für USB-Flashlaufwerk • Steuerung der Serverstromversorgung und -Grundstellung im Fenster "Fernsteuerung" • Anzeige im Fenster "Fernsteuerung" kann in einer Datei gespeichert werden Das IMM stellt zwei separate Clientfenster bereit. Ein Fenster ist für Bildschirm-, Tastatur- und Mausinteraktionen vorgesehen, das andere für virtuelle Datenträger. Die IMM-Webschnittstelle bietet eine Menüoption, die es ermöglicht, die Farbtiefe anzupassen, um bei geringer Bandbreite die übertragene Datenmenge zu verringern. Die Schnittstelle des Remote Supervisor Adapter II verfügt über eine Schiebeleiste für die Bandbreite.
Sicherheit	Der Remote Supervisor Adapter II verfügt über erweiterte Sicherheitsfunktionen, einschließlich SSL (Secure Sockets Layer) und Verschlüsselung.	Das IMM weist dieselben Sicherheitsfunktionen wie der Remote Supervisor Adapter II auf.

Tabelle 1. Vergleich der IMM-Produktmerkmale mit den kombinierten Produktmerkmalen des BMC und des Remote Supervisor Adapter II in System x Servern (Forts.)

Beschreibung	BMC mit Remote Supervisor Adapter II	IMM
Serielle Umleitung	Die IPMI-SOL-Funktion (Serial over LAN) ist eine Standardfunktion des BMC. Der Remote Supervisor Adapter II ermöglicht das Umleiten von seriellen Serverdaten in eine Telnet- oder SSH-Sitzung. **Anmerkung:** Diese Funktion ist nicht auf allen Servern verfügbar.	Der Anschluss COM1 wird auf System x Servern für SOL verwendet. COM1 kann nur über die IPMI-Schnittstelle konfiguriert werden. Der Anschluss COM2 wird für serielle Umleitungen über Telnet oder SSH verwendet. COM2 kann über alle IMM-Schnittstellen konfiguriert werden, mit Ausnahme der IPMI-Schnittstelle. Der Anschluss COM2 wird auf Blade-Servern für SOL verwendet. Beide COM-Anschlusskonfigurationen sind auf 8 Datenbit, Parität null, 1 Stoppbit und eine Baudrateauswahl von 9600, 19200, 38400, 57600, 115200 oder 230400 beschränkt. Auf Blade-Servern ist der Anschluss COM2 ein interner COM-Anschluss ohne die Möglichkeit eines externen Zugriffs. Auf Blade-Servern ist die gemeinsame Nutzung des seriellen IPMI-Anschlusses nicht möglich. Auf in einem Gehäuse installierten Servern und auf Turmservern ist der IMM-Anschluss COM2 ein interner COM-Anschluss ohne die Möglichkeit eines externen Zugriffs.
SNMP	Die SNMP-Unterstützung ist auf SNMPv1 begrenzt.	Das IMM unterstützt SNMPv1 und SNMPv3.

IMM mit einem erweiterten BladeCenter-Managementmodul verwenden

Das erweitertes BladeCenter-Managementmodul ist die Standardschnittstelle für Systemmanagement in IBM BladeCenter- und IBM Blade-Servern. Obwohl das IMM inzwischen in einigen IBM BladeCenter- und IBM Blade-Servern enthalten ist, bleibt das erweiterte Managementmodul das Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für BladeCenter- und Blade-Server. Die externen Netzschnittstellen zum IMM sind im BladeCenter nicht verfügbar.

Auf Blade-Servern gibt es keinen externen Netzzugriff auf das IMM. Für die Fernverwaltung von Blade-Servern muss das erweiterte Managementmodul verwendet werden. Das IMM ersetzt die Funktionalität des BMC der cKVM-Erweiterungskarte (Concurrent Keyboard, Video and Mouse - cKVM) in früheren Blade-Server-Produkten.

Voraussetzungen - Web-Browser und Betriebssystem

Für die IMM-Webschnittstelle sind das Java™-Plug-in ab Version 1.5 (für die Remote-Presence-Funktion) und einer der folgenden Web-Browser erforderlich:

- Microsoft Internet Explorer Version 6.0, 7.0 oder 8.0 mit dem aktuellen Service-Pack. Versionen nach 8.0 werden nicht unterstützt.
- Mozilla Firefox ab Version 1.5

Die folgenden Serverbetriebssysteme bieten USB-Unterstützung, die für die Remote-Presence-Funktion erforderlich ist:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux, Version 4.0 und 5.0
- SUSE Linux Version 10.0
- Novell NetWare 6.5

Anmerkung: Die IMM-Webschnittstelle unterstützt keine Sprachen mit Doppelbytezeichensatz.

Bemerkungen in diesem Buch

In dieser Dokumentation werden die folgenden Bemerkungen verwendet:

- **Anmerkung:** Diese Bemerkungen enthalten wichtige Tipps, Anleitungen oder Ratschläge.
- **Wichtig:** Diese Bemerkungen enthalten Informationen oder Ratschläge, die Ihnen helfen, schwierige oder problematische Situationen zu vermeiden.
- **Achtung:** Diese Bemerkungen weisen auf die Gefahr der Beschädigung von Programmen, Einheiten oder Daten hin. Eine Bemerkung vom Typ "Achtung" befindet sich direkt vor der Anweisung oder der Beschreibung der Situation, die diese Beschädigung bewirken könnte.

Kapitel 2. IMM-Webschnittstelle öffnen und verwenden

Das IMM kombiniert Serviceprozessorfunktionen, einen Videocontroller und eine Remote Presence-Funktion (wenn ein optionaler Virtual Media Key installiert ist) in einem einzigen Chip. Für einen Fernzugriff auf das IMM mithilfe der IMM-Webschnittstelle müssen Sie sich zuerst anmelden. In diesem Kapitel werden das Anmeldeverfahren und die Aktionen beschrieben, die Sie über die IMM-Webschnittstelle ausführen können.

Zugriff auf die IMM-Webschnittstelle

Das IMM unterstützt eine statische IPv4-Adressierung wie auch eine DHCP-IPv4-Adressierung. Die statische IPv4-Standardadresse, die dem IMM zugeordnet wird, lautet 192.168.70.125. Das IMM ist anfangs so konfiguriert, dass es versucht, eine Adresse von einem DHCP-Server abzurufen. Ist dies nicht möglich, verwendet es die statische IPv4-Adresse.

Das IMM unterstützt auch IPv6, aber es verfügt standardmäßig nicht über eine festgelegte statische IPv6-IP-Adresse. Beim Erstzugriff auf das IMM in einer IPv6-Umgebung können Sie entweder die IPv4-IP-Adresse oder die lokale IPv6-Verbindungsadresse verwenden. Das IMM generiert eine eindeutige lokale IPv6-Verbindungsadresse, die in der IMM-Webschnittstelle auf der Seite "Network Interfaces" (Netzschnittstellen) angezeigt wird. Die lokale IPv6-Verbindungsadresse weist dabei dasselbe Format auf, das im folgenden Beispiel dargestellt ist.

```
fe80::21a:64ff:fee6:4d5
```

Beim Zugriff auf das IMM sind die folgenden IPv6-Bedingungen als Standardwerte definiert:

- Die automatische IPv6-Adressenkonfiguration ist aktiviert.
- Die statische IPv6-IP-Adressenkonfiguration ist inaktiviert.
- DHCPv6 ist aktiviert.
- Die statusunabhängige automatische Konfiguration ist aktiviert.

Das IMM ermöglicht die Auswahl einer dedizierten Systemmanagementnetzverbindung (falls vorhanden) oder einer Netzverbindung, die gemeinsam mit dem Server verwendet wird. Die Standardverbindung für in einem Gehäuserahmen installierte Server und Turmserver verwendet den dedizierten Systemmanagementnetzanschluss.

Anmerkung: Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze. Wenn auf Ihrer Hardware kein Anschluss für dedizierte Netze vorhanden ist, ist die Einstellung *Shared* (Gemeinsam genutzt) die einzig verfügbare IMM-Einstellung.

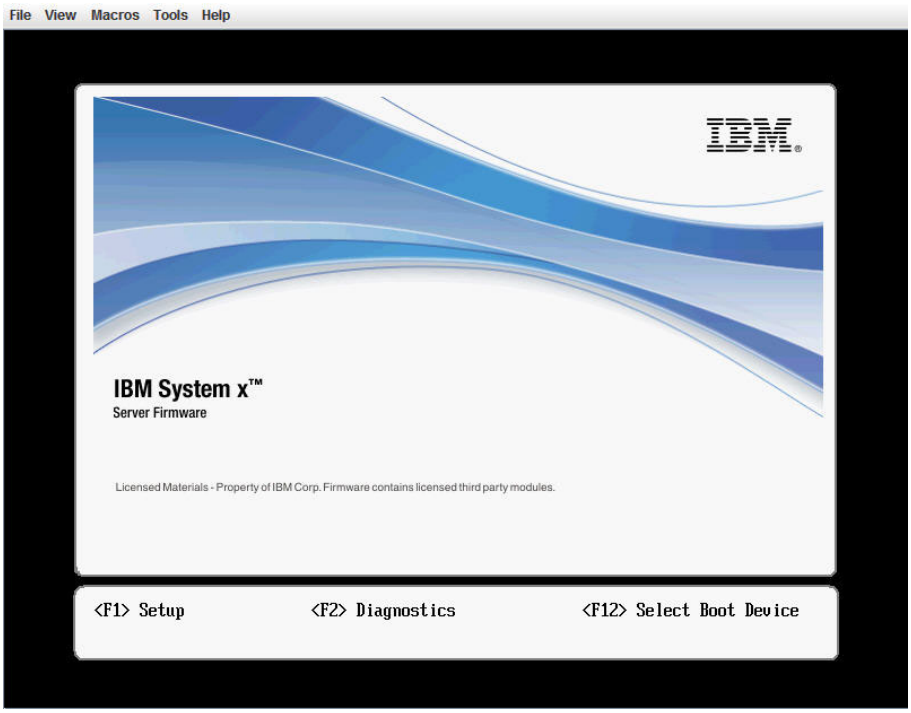
Einrichten der IMM-Netzverbindung mit dem Konfigurationsdienstprogramm der Server-Firmware für IBM System x

Nachdem Sie den Server gestartet haben, können Sie über das Konfigurationsdienstprogramm eine IMM-Netzverbindung auswählen. Der Server mit der IMM-Hardware muss mit einem Dynamic Host Configuration Protocol-Server (DHCP) verbunden sein oder das Servernetz muss so konfiguriert sein, dass es die statische

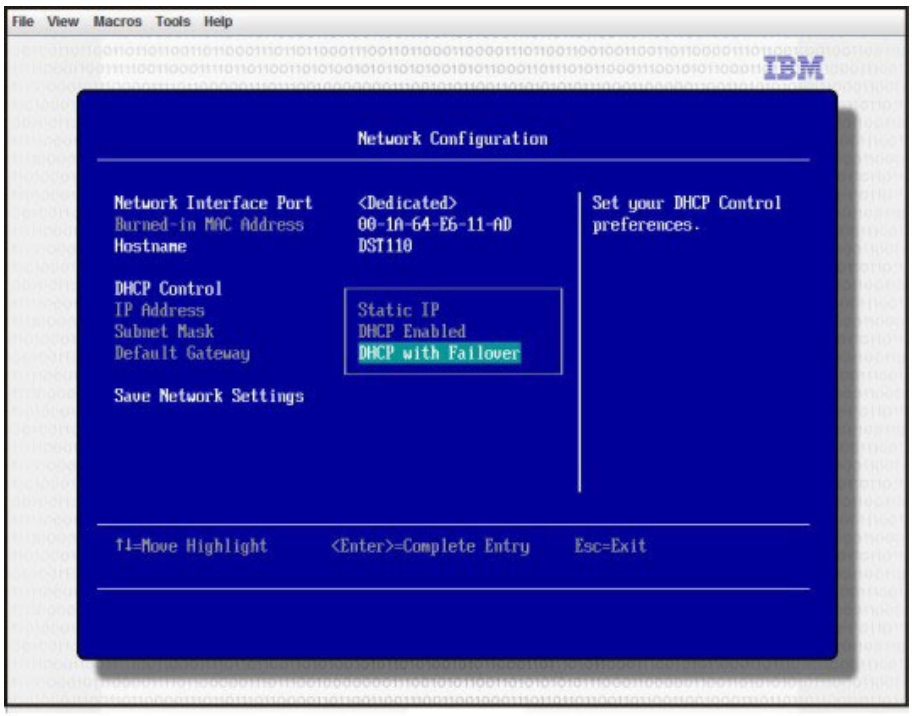
IMM-IP-Adresse verwendet. Gehen Sie wie folgt vor, um die IMM-Netzverbindung über das Konfigurationsdienstprogramm herzustellen:

1. Schalten Sie den Server ein. Die Eingangsanzeige der Server-Firmware für IBM System x wird angezeigt.

   Anmerkung: Der Netzschalter wird etwa 2 Minuten nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.



2. Wenn die Aufforderung `<F1> Setup` (F1 für Konfiguration) angezeigt wird, drücken Sie die Taste F1. Wenn Sie sowohl ein Startkennwort als auch ein Administratorkennwort festgelegt haben, müssen Sie das Administratorkennwort eingeben, um auf das vollständige Menü des Konfigurationsdienstprogramms zugreifen zu können.
3. Wählen Sie im Hauptmenü des Konfigurationsdienstprogramms **System Settings** (Systemeinstellungen) aus.
4. Wählen Sie in der nächsten Anzeige die Option **Integrated Management Module** aus.
5. Wählen Sie in der nächsten Anzeige die Option **Network Configuration** (Netzkonfiguration) aus.
6. Markieren Sie **DHCP Control**. Im Feld **DHCP Control** stehen drei IMM-Netzverbindungen zur Auswahl:
   - Static IP
   - DHCP Enabled (DHCP aktiviert)
   - DHCP with Failover (default) (DHCP mit Funktionsübernahme (Standard))



7. Wählen Sie eine der Netzverbindungen.
8. Wenn Sie sich dafür entscheiden, eine statische IP-Adresse zu verwenden, müssen Sie die IP-Adresse, die Teilnetzmaske und das Standard-Gateway angeben.
9. Sie können das Konfigurationsdienstprogramm auch dazu verwenden, eine dedizierte Netzverbindung (wenn Ihr Server einen Anschluss für dedizierte Netze hat) oder eine freigegebene IMM-Netzverbindung auszuwählen.

   Anmerkungen:

   - Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze. Wenn auf Ihrer Hardware kein Anschluss für dedizierte Netze vorhanden ist, ist die Einstellung *shared* (gemeinsam genutzt) die einzig verfügbare IMM-Einstellung. Wählen Sie auf der Anzeige **Network Configuration** im Feld **Network Interface Port** (Netzschnittstellenanschluss) **Dedicated** (dediziert) (falls zutreffend) oder **Shared** (gemeinsam genutzt) aus.
   - Informationen dazu, wo sich auf Ihrem Server die vom IMM genutzten Ethernet-Anschlüsse befinden, bekommen Sie in der Dokumentation, die im Lieferumfang Ihres Servers enthalten war.
10. Wählen Sie **Save Network Settings** (Netzeinstellungen speichern).
11. Beenden Sie das Konfigurationsdienstprogramm.

Anmerkungen:

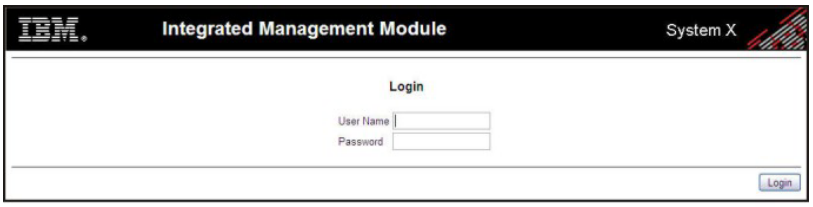
- Sie müssen etwa eine Minute warten, bis die Änderungen wirksam werden und die Server-Firmware wieder funktioniert.
- Sie können die IMM-Netzverbindung auch über die IMM-Webschnittstelle konfigurieren. Weitere Informationen finden Sie im Abschnitt „Netzschnittstellen konfigurieren” auf Seite 41.

Anmeldung am IMM

Wichtiger Hinweis: Das IMM ist anfangs auf den Benutzernamen `USERID` und das Kennwort `PASSW0RD` (mit einer Null anstelle des Buchstaben "O") eingestellt. Bei dieser Standard-Benutzereinstellung haben nur Administratoren Zugriff. Ändern Sie für größere Sicherheit dieses Standardkennwort bei der Erstkonfiguration.

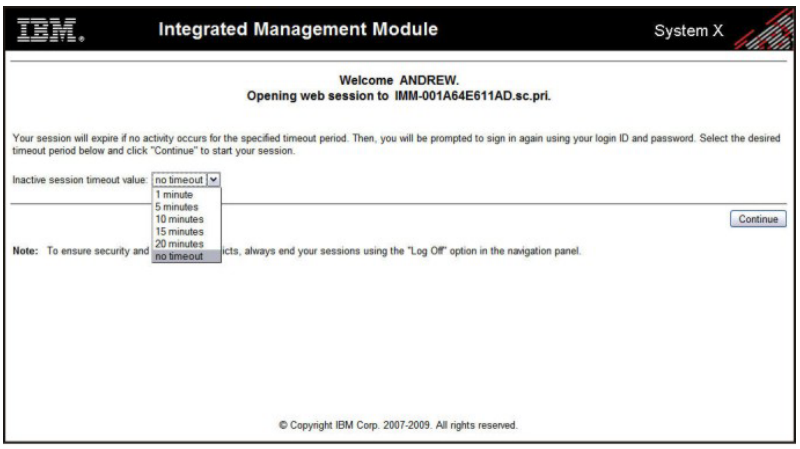
Gehen Sie wie folgt vor, um über die IMM-Webschnittstelle Zugriff auf das IMM zu bekommen:

1. Öffnen Sie einen Web-Browser. Geben Sie im Adress- oder URL-Feld die IP-Adresse oder den Hostnamen des IMM-Servers ein, mit dem Sie eine Verbindung herstellen möchten.

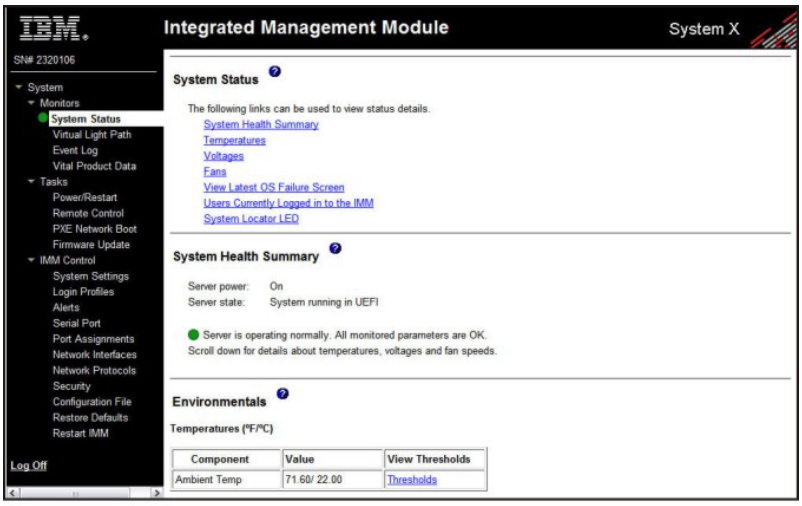


2. Geben Sie Ihren Benutzernamen und Ihr Kennwort in das Fenster "Login" (Anmelden) des IMM ein. Wenn Sie das IMM zum ersten Mal verwenden, können Sie Ihren Benutzernamen und Ihr Kennwort von Ihrem Systemadministrator anfordern. Alle Anmeldeversuche werden im Ereignisprotokoll dokumentiert. Je nachdem, wie Ihr Systemadministrator die Benutzer-ID konfiguriert hat, müssen Sie möglicherweise ein neues Kennwort eingeben.
3. Wählen Sie auf der Willkommen-Webseite ein Zeitlimit aus der Dropdown-Liste im angegebenen Feld. Wenn Ihr Browser diese Anzahl an Minuten inaktiv ist, meldet das IMM Sie von der Webschnittstelle ab.

   Anmerkung: Je nachdem, wie Ihr Systemadministrator die allgemeinen Anmeldungseinstellungen konfiguriert hat, kann es sich bei diesem Zeitlimit auch um einen vorgegebenen Wert handeln.



4. Klicken Sie auf **Continue** (Fortfahren), um die Sitzung zu starten. Der Browser öffnet die Seite "System Status", die Ihnen einen schnellen Überblick über den Serverstatus und die Zusammenfassung des Serverzustands bietet.



Beschreibungen der Aktionen, die Sie über die Links im linken Navigationsfenster ausführen können, finden Sie im Abschnitt „Beschreibung von IMM-Aktionen". Gehen Sie dann weiter zu Kapitel 3, „IMM konfigurieren", auf Seite 21.

Beschreibung von IMM-Aktionen

In Tabelle 2 sind die Aktionen aufgelistet, die bei einer Anmeldung am IMM verfügbar sind.

Tabelle 2. IMM-Aktionen

Link	Maßnahme	Beschreibung
System Status (Systemstatus)	Systemzustand eines Servers anzeigen; Anzeigenerfassung bei einem Systemabsturz anzeigen; am IMM angemeldete Benutzer anzeigen	Auf der Seite "System Health" (Systemzustand) können Sie die Serverstromversorgung und den Serverstatus, die Temperatur, die Spannung und den Lüfterstatus Ihres Servers überwachen. Sie können außerdem das Bild der letzten Anzeigenerfassung bei einem Systemabsturz und die derzeit am IMM angemeldeten Benutzer anzeigen.
Virtual Light Path	Den Namen, die Farbe und den Status der einzelnen Anzeigen im Diagnosefeld "Light Path Diagnostics" des Servers anzeigen	Auf der Seite "Virtual Light Path" wird der aktuelle Status der Anzeigen am Server angezeigt.
Event Log (Ereignisprotokoll)	Ereignisprotokolle für ferne Server anzeigen	Die Seite "Event Log" enthält Einträge, die derzeit im Gehäuseereignisprotokoll gespeichert sind. Das Protokoll enthält eine Textbeschreibung der Ereignisse, die vom BMC gemeldet wurden, und Informationen zu allen Fernzugriffversuchen sowie zu allen Konfigurationsänderungen. Alle Ereignisse im Protokoll sind mit einer Zeitmarke gekennzeichnet, die die IMM-Einstellungen für Datum und Uhrzeit verwendet. Einige Ereignisse generieren außerdem Alerts, falls dies auf der Seite "Alerts" so konfiguriert wurde. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern.
Vital Product Data (elementare Produktdaten)	Elementare Produktdaten (VPD) des Servers anzeigen	Das IMM erfasst Serverinformationen, Server-Firmwareinformationen und elementare Produktdaten von Serverkomponenten. Diese Daten sind auf der Seite "Vital Product Data" verfügbar.

Tabelle 2. IMM-Aktionen (Forts.)

Link	Maßnahme	Beschreibung
Power/Restart (Einschalten/ Neustart)	Einen Server über Fernzugriff einschalten oder erneut starten	Das IMM stellt eine vollständige Fernsteuerung der Stromversorgung Ihres Servers bereit, einschließlich Aktionen zu Einschalten, Ausschalten und erneut Starten. Außerdem werden die Statistikdaten zum Einschalten und Neustart erfasst und angezeigt, um die Verfügbarkeit der Server-Hardware anzugeben.
Remote Control (Fernsteuerung)	Server-Videokonsole umleiten und ein Computerplattenlaufwerk oder ein Plattenimage als Laufwerk für den Server verwenden	Auf der Seite "Remote Control" können Sie die Fernsteuerungsfunktion starten. Mithilfe der Fernsteuerung können Sie die Serverkonsole von Ihrem Computer aus anzeigen und eines Ihrer Computerplattenlaufwerke, wie z. B. das CD-ROM-Laufwerk oder das Diskettenlaufwerk, über eine Mountoperation an den Server anhängen. Sie können Ihre Maus und Tastatur für Interaktionen auf dem Server und für die Steuerung des Servers verwenden. Wenn Sie einen Datenträger angehängt haben, können Sie ihn für einen Neustart des Servers sowie für die Aktualisierung der Firmware auf dem Server verwenden. Das angehängte Laufwerk wird als an den Server angeschlossenes USB-Plattenlaufwerk angezeigt.
PXE Network Boot (PXE-Netzboot)	Startreihenfolge (Bootreihenfolge) des Host-Servers für den nächsten Neustart ändern, um einen PXE/ DHCP-Netzstart (Preboot Execution Environment/Dynamic Host Configuration Protocol) zu versuchen	Wenn Ihre Server-Firmware und das Dienstprogramm "PXE Boot Agent" richtig definiert sind, können Sie auf der Seite "PXE Network Boot" die Startreihenfolge (Bootreihenfolge) des Hostservers für den nächsten Neustart ändern, um zu versuchen, einen PXE/DHCP-Netzstart durchzuführen. Die Host-Startreihenfolge wird nur geändert, wenn für den Host kein privilegierter Zugriffsschutz (Privileged Access Protection, PAP) festgelegt ist. Nach dem nächsten Neustart wird die Auswahl des Kontrollkästchens auf der Seite "PXE Network Boot" aufgehoben.
Firmware Update (Firmwareaktualisierung)	Firmware auf dem IMM aktualisieren	Aktualisieren Sie mithilfe der Optionen auf der Seite "Firmware Update" die IMM-Firmware, die Server-Firmware und die DSA-Firmware.
System Settings (Systemeinstellungen)	IMM-Servereinstellungen anzeigen und ändern	Auf der Seite "System Settings" können Sie den Serverstandort und allgemeine Informationen konfigurieren, wie z. B. den Namen des IMM, die Einstellungen für eine Zeitlimitüberschreitung des Servers und die Kontaktinformationen für das IMM.
	IMM-Taktgeber einstellen	Sie können den IMM-Taktgeber einstellen, mit dem die Zeitmarken der Einträge im Ereignisprotokoll erstellt werden.
	USB-Inband-Schnittstelle aktivieren oder inaktivieren	Sie können die USB-Inband-Schnittstelle (oder LAN over USB) aktivieren oder inaktivieren.
Login Profiles (Anmeldeprofile)	IMM-Anmeldeprofile und globale Anmeldeeinstellungen konfigurieren	Sie können bis zu 12 Anmeldeprofile definieren, die einen Zugriff auf das IMM ermöglichen. Sie können außerdem globale Anmeldeeinstellungen definieren, die für alle Anmeldeprofile gelten, einschließlich der Aktivierung einer LDAP-Serverauthentifizierung (Lightweight Directory Access Protocol) und der Anpassung der Kontensicherheitsstufe.

Tabelle 2. IMM-Aktionen (Forts.)

Link	Maßnahme	Beschreibung
Alerts	Ferne Alerts und Empfänger von fernen Alerts konfigurieren	Sie können das IMM so konfigurieren, dass es Alerts zu verschiedenen Ereignissen generiert und weiterleitet. Auf der Seite "Alerts" können Sie die Alerts, die überwacht werden sollen, und die Empfänger, die benachrichtigt werden sollen, konfigurieren.
	SNMP-Ereignisse (Simple Network Management Protocol) konfigurieren	Sie können die Ereigniskategorien festlegen, für die SNMP-Traps gesendet werden.
	Alerteinstellungen konfigurieren	Sie können globale Einstellungen festlegen, die für alle fernen Alertempfänger gelten, wie z. B. die Anzahl an Alertneuversuchen und die Verzögerung zwischen den Neuversuchen.
Serial Port (Serieller Anschluss)	Einstellungen für den seriellen Anschluss des IMM konfigurieren	Auf der Seite "Serial Port" können Sie die Baudrate des seriellen Anschlusses konfigurieren, der von der seriellen Umleitungsfunktion verwendet wird. Sie können außerdem die Tastenkombination für den Wechsel zwischen den Modi der seriellen Umleitung und der Befehlszeilenschnittstelle (CLI) konfigurieren.
Port assignments (Portzuordnungen)	Portnummern der IMM-Protokolle ändern	Auf der Seite "Port Assignments" können Sie die Portnummern anzeigen und ändern, die den IMM-Protokollen zugeordnet sind (wie z. B. HTTP, HTTPS, Telnet und SNMP).
Network Interfaces (Netzschnittstellen)	Netzschnittstellen des IMM konfigurieren	Auf der Seite "Network Interfaces" (Netzschnittstellen) können Sie die Einstellungen für den Netzzugriff für die Ethernet-Verbindung zum IMM einrichten.
Network Protocols (Netzprotokolle)	Netzprotokolle des IMM konfigurieren	Auf der Seite "Network Protocols" können Sie die Einstellungen für SNMP (Simple Network Management Protocol), DNS (Domain Name System) und SMTP (Simple Mail Transfer Protocol) konfigurieren, die vom IMM verwendet werden. Sie können außerdem die LDAP-Parameter konfigurieren.
Security (Sicherheit)	SSL (Secure Sockets Layer) konfigurieren	Sie können SSL aktivieren oder inaktivieren und die verwendeten SSL-Zertifikate verwalten. Außerdem können Sie aktivieren oder inaktivieren, ob eine SSL-Verbindung für Verbindungen zu einem LDAP-Server erforderlich ist.
	SSH-Zugriff (Secure Shell) aktivieren	Sie können einen SSH-Zugriff auf das IMM aktivieren.
Configuration File (Konfigurationsdatei)	IMM-Konfiguration sichern und wiederherstellen	Auf der Seite "Configuration File" können Sie die Konfiguration des IMM sichern, ändern und wiederherstellen und eine Konfigurationszusammenfassung anzeigen.
Restore Default Settings (Standardeinstellungen wiederherstellen)	IMM-Standardeinstellungen wiederherstellen	**Achtung:** Wenn Sie auf **Restore Defaults** klicken, verlieren Sie sämtliche Änderungen, die Sie am IMM vorgenommen haben. Sie können die Konfiguration des IMM auf die werkseitigen Voreinstellungen zurücksetzen.
Restart IMM (IMM erneut starten)	IMM erneut starten	Sie können das IMM erneut starten.

Tabelle 2. IMM-Aktionen (Forts.)

Link	Maßnahme	Beschreibung
Scalable Partitioning (Skalierbare Partitionierung)	Den Server als Partition in einem skalierbaren Komplex konfigurieren	Wenn der Server in einem skalierbaren Komplex konfiguriert wird, können Sie das System mithilfe des IMM auch in diesem Komplex steuern. Wenn ein Fehler hinsichtlich der Skalierbarkeit des Servers auftritt, meldet das IMM einen entsprechenden Fehler.
Service Advisor	Wartungsfähige Ereigniscodes an den IBM Support weiterleiten	Wenn der Service Advisor aktiviert ist, ermöglicht er dem IMM wartungsfähige Ereigniscodes für eine weitere Fehlerbehebung an den IBM Support weiterzuleiten. **Anmerkung:** Informationen dazu, ob Ihr Server diese Funktion unterstützt, finden Sie in der Dokumentation zu Ihrem Server.
Log off (Abmelden)	Vom IMM abmelden	Sie können die Verbindung zum IMM beenden und sich vom IMM abmelden.

Klicken Sie auf den Link **View Configuration Summary** (Konfigurationszusammenfassung anzeigen), der sich oben rechts auf den meisten Seiten befindet, um die Konfiguration des IMM schnell aufzurufen.

Kapitel 3. IMM konfigurieren

Mithilfe der Links unter **IMM Control** (IMM-Steuerung) im Navigationsfenster können Sie das IMM konfigurieren.

Auf der Seite "System Settings" (Systemeinstellungen) können Sie folgende Tasks ausführen:

- Serverinformationen festlegen
- Serverzeitlimits festlegen
- Datum und Uhrzeit für das IMM festlegen
- Befehle für die USB-Schnittstelle aktivieren oder inaktivieren

Auf den Seite "Login Profiles" (Anmeldeprofile) können Sie folgende Tasks ausführen:

- Anmeldeprofile festlegen, um den Zugriff auf das IMM zu steuern
- Globale Anmeldeeinstellungen konfigurieren, wie z. B. die Aussperrungszeit nach nicht erfolgreichen Anmeldeversuchen
- Kontensicherheitsstufe konfigurieren

Auf der Seite "Alerts" können Sie folgende Tasks ausführen:

- Empfänger der fernen Alerts konfigurieren
- Anzahl der fernen Alertversuche festlegen
- Verzögerung zwischen Alerts auswählen
- Alerttyp und Art der Weiterleitung auswählen

Auf den Seite "Serial Port" (Serieller Anschluss) können Sie folgende Tasks ausführen:

- Baudrate des serieller Anschlusses 2 (COM2) für eine serielle Umleitung konfigurieren
- Tastenfolge für den Wechsel zwischen serieller Umleitung und Befehlszeilenschnittstelle (CLI) angeben

Auf der Seite "Port Assignments" (Anschlusszuordnungen) können Sie die Anschlussnummern der IMM-Services ändern.

Auf der Seite "Network Interfaces" (Netzschnittstellen) können Sie die Ethernet-Verbindung für das IMM einrichten.

Auf der Seite "Network Protocols" können Sie Folgendes konfigurieren:

- SNMP-Konfiguration
- DNS-Konfiguration
- Telnet-Protokoll
- SMTP-Konfiguration
- LDAP-Konfiguration
- Service Location Protocol

Auf der Seite "Security" (Sicherheit) können Sie die SSL-Einstellungen (Secure Sockets Layer) installieren und konfigurieren.

Auf der Seite "Configuration File" (Konfigurationsdatei) können Sie die Konfiguration des IMM sichern, ändern und wiederherstellen.

Auf der Seite "Restore Defaults" (Standardwerte wiederherstellen) können Sie die IMM-Konfiguration auf die werkseitigen Voreinstellungen zurücksetzen.

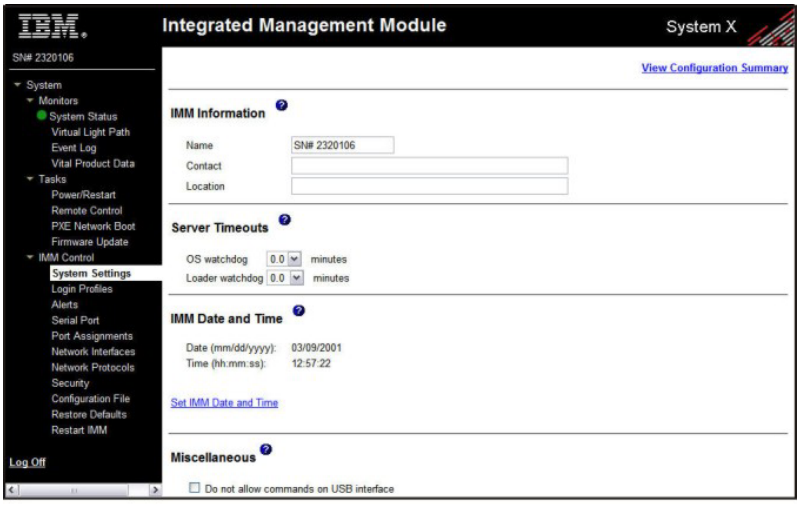
Auf der Seite "Restart IMM" (IMM-Neustart) können Sie das IMM erneut starten.

Einstellung von Systeminformationen

Gehen Sie wie folgt vor, um die IMM-Systeminformationen einzustellen:

1. Melden Sie sich an dem IMM an, für das Sie die Systeminformationen einstellen möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **System Settings** (Systemeinstellungen). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

   Anmerkung: Welche Felder auf der Seite "System Settings" (Systemeinstellungen) verfügbar sind, hängt vom fernen Server ab, auf den zugegriffen wird.



3. Geben Sie im Feld **Name** im Bereich **IMM Information** den Namen des IMM ein. Verwenden Sie das Feld **Name**, um einen Namen für das IMM in diesem Server anzugeben. Der Name wird in E-Mail- und SNMP-Alertbenachrichtigungen (Simple Network Management Protocol) angeführt, um die Quelle des Alerts anzugeben.

   Anmerkung: Ihr IMM-Name (im Feld **Name**) und der IP-Hostname des IMM (im Feld **Hostname** auf der Seite "Network Interfaces" (Netzschnittstellen)) lauten nicht automatisch gleich, da das Feld **Name** auf 16 Zeichen begrenzt ist. Im Feld **Hostname** können bis zu 63 Zeichen stehen. Um Verwirrung möglichst zu vermeiden, legen Sie das Feld **Name** als nichtqualifizierten Teil des IP-Hostnamens fest. Der nichtqualifizierte IP-Hostname besteht aus den Zeichen vor dem ersten Punkt des vollständig qualifizierten IP-Hostnamens. Beispiel: Beim vollständig qualifizierten IP-Hostnamen "imm1.us.company.com" lautet der nichtqualifizierte IP-Hostname "imm1". Informationen zu Ihrem Hostnamen finden Sie im Abschnitt „Netzschnittstellen konfigurieren” auf Seite 41.

4. Geben Sie im Feld **Contact** die Kontaktinformationen ein. Sie können beispielsweise Name und Telefonnummer der Person angeben, die im Falle eines Problems mit diesem Server der Ansprechpartner ist. Sie können in dieses Feld höchstens 47 Zeichen eingeben.
5. Geben Sie im Feld **Location** den Standort des Servers an. Machen Sie in diesem Feld auch Angaben, die detailliert genug sind, um den Server zu Wartungs- oder anderen Zwecken schnell lokalisieren zu können. Sie können in dieses Feld höchstens 47 Zeichen eingeben.
6. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save**.

Serverzeitlimits festlegen

Anmerkung: Bei Serverzeitlimits muss die Inband-USB-Schnittstelle (oder LAN over USB) aktiviert sein, um Befehle zuzulassen. Weitere Informationen zu den Aktivierungs- und Inaktivierungsbefehlen für die USB-Schnittstelle finden Sie im Abschnitt „USB-Inband-Schnittstelle inaktivieren" auf Seite 26. Weitere Informationen zur Installation des erforderlichen Einheitentreibers finden Sie im Abschnitt „Einheitentreiber installieren" auf Seite 144.

Gehen Sie wie folgt vor, um die Werte für das Serverzeitlimit festzulegen:

1. Melden Sie sich an dem IMM an, für das Sie die Serverzeitlimits festlegen möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **System Settings** (Systemeinstellungen) und blättern Sie abwärts zum Bereich **Server Timeouts** (Serverzeitlimits).

   Sie können das IMM so einstellen, dass es automatisch auf die folgenden Ereignisse reagiert:

   - Das Betriebssystem läuft in einer Endlosschleife
   - Das Betriebssystem wird nicht geladen
3. Aktivieren Sie die Serverzeitlimits, die den Ereignissen entsprechen, auf die das IMM automatisch reagieren soll.

   OS watchdog (Watchdog für das Betriebssystem)
   Verwenden Sie das Feld **OS watchdog**, um die Anzahl an Minuten zwischen Prüfungen des Betriebssystems durch das IMM anzugeben. Wenn das Betriebssystem auf eine dieser Prüfungen nicht reagiert, generiert das IMM einen Betriebssystem-Zeitlimitalert und startet den Server erneut. Nach dem Neustart des Servers ist der Betriebssystem-Watchdog inaktiviert, bis das Betriebssystem heruntergefahren und der Server aus- und wieder eingeschaltet wird.

   Wählen Sie zum Festlegen des Wertes für den Betriebssystem-Watchdog ein Zeitintervall aus dem Menü aus. Zum Ausschalten dieses Watchdogs wählen Sie **0.0** aus dem Menü. Zum Aufzeichnen von Betriebssystemfehleranzeigen müssen Sie den Watchdog im Feld **OS watchdog** aktivieren.

   Loader watchdog (Watchdog für das Ladeprogramm)
   Verwenden Sie das Feld **Loader watchdog**, um anzugeben, wie viele Minuten das IMM zwischen der Fertigstellung des POST und dem Starten des Betriebssystems warten soll. Wenn diese Zeitspanne überschritten wird, generiert das IMM einen Ladeprogramm-Zeitlimitalert und startet den Server automatisch erneut. Nach dem Neustart des Servers wird das Ladeprogramm-Zeitlimit automatisch inaktiviert, bis das Be-

triebssystem heruntergefahren und der Server aus- und wieder eingeschaltet wird (oder bis das Betriebssystem startet und die Software erfolgreich geladen wird).

Zum Festlegen des Wertes für das Ladeprogramm-Zeitlimit wählen Sie, wie lange das IMM auf die Fertigstellung des Betriebssystemstarts warten soll. Zum Ausschalten dieses Watchdogs wählen Sie **0.0** aus dem Menü.

Power off delay (Ausschaltverzögerung)
Verwenden Sie das Feld **Power off delay**, um anzugeben, wie viele Minuten das IMM darauf warten soll, dass das Betriebssystem herunterfährt, bevor es die Stromversorgung des Servers ausschaltet (sofern die Stromversorgung nicht bereits durch das Betriebssystem selbst ausgeschaltet wurde). Wenn Sie die Ausschaltverzögerung einstellen, können Sie sicherstellen, dass das Betriebssystem genug Zeit für einen ordnungsgemäßen Systemabschluss hat, bevor die Stromversorgung des Servers ausgeschaltet wird. Um die Ausschaltverzögerung für Ihren Server festzulegen, fahren Sie Ihren Server herunter und stellen Sie fest, wie viel Zeit das Herunterfahren in Anspruch nimmt. Fügen Sie dieser Zeit einen Zeitpuffer hinzu und verwenden Sie die sich ergebende Zeitspanne als Einstellung für Ihre Ausschaltverzögerung.

Zum Festlegen des Wertes für die Ausschaltverzögerung wählen Sie den gewünschten Zeitwert aus dem Menü aus. Der Wert X'0' bedeutet, dass das Betriebssystem und nicht das IMM die Stromversorgung des Servers ausschaltet.

4. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save**.

Datum und Uhrzeit für IMM einstellen

Das IMM verwendet einen eigenen Taktgeber, um alle Ereignisse im Ereignisprotokoll zeitlich zu markieren.

Anmerkung: Die Datums- und Uhrzeiteinstellung des IMM wirkt sich nur auf die IMM-Uhr und nicht auf die Serveruhr aus. Bei IMM-Taktgeber und Serveruhr handelt es sich um separate, voneinander unabhängige Uhren, die auf unterschiedliche Uhrzeiten eingestellt werden können. Gehen Sie zum Synchronisieren von IMM-Uhr und Serveruhr in den Bereich **Network Time Protocol** der Seite und stellen Sie den Server-Hostnamen des NTP (Network Time Protocol) auf den gleichen Server-Hostnamen bzw. die gleiche IP-Adresse ein, die verwendet wird, um die Serveruhr einzustellen. Weitere Informationen finden Sie im Abschnitt „Synchronisation von Taktgebern in einem Netz" auf Seite 25.

Bei Alerts, die per E-Mail und SNMP versendet werden, wird die Taktgebereinstellung zur zeitlichen Markierung verwendet. Zwecks größerer Benutzerfreundlichkeit für Administratoren, die über Fernzugriff Systeme in unterschiedlichen Zeitzonen verwalten, werden Ausgleiche der westeuropäischen Zeit und die Sommerzeit von den Zeiteinstellungen unterstützt. Sie können selbst dann über Fernzugriff auf das Ereignisprotokoll zugreifen, wenn der Server ausgeschaltet oder inaktiviert ist.

Gehen Sie wie folgt vor, um die Datums- und Zeiteinstellungen des IMM zu überprüfen:

1. Melden Sie sich an dem IMM an, für das Sie die IMM-Datums- und Zeitangaben festlegen möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.

2. Klicken Sie im Navigationsfenster auf **System Settings** (Systemeinstellungen) und blättern Sie abwärts zum Bereich **IMM Date and Time** (IMM-Datum und -Uhrzeit), der Datum und Uhrzeit der Webseitenerstellung anzeigt.
3. Zum Überschreiben der Datums- und Uhrzeiteinstellungen und zum Aktivieren des Ausgleichs von Sommerzeit und westeuropäischer Zeit klicken Sie auf **Set IMM Date and Time** (IMM-Datum und -Uhrzeit einstellen). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

4. Geben Sie im Feld **Date** die Zahlen des laufenden Monats, Tages und Jahres ein.
5. Geben Sie im Feld **Time** in den entsprechenden Eingabefeldern die Zahlen ein, die der laufenden Stunde, Minute und Sekunde entsprechen. Bei Stunde (hh) muss eine Zahl zwischen 00 und 23 stehen, wie sie bei einer 24-Stunden-Zeiteinteilung dargestellt sind. Bei Minuten (mm) und Sekunden (ss) müssen Zahlen zwischen 00 und 59 stehen.
6. Wählen Sie im Feld **GMT offset** (GMT-Abstand) die Zahl aus, die den Abstand in Stunden zur westeuropäischen Zeit angibt, entsprechend der Zeitzone, in der sich der Server befindet.
7. Wählen Sie das Kontrollkästchen **Automatically adjust for daylight saving changes** (Automatisch an Sommerzeit anpassen) oder wählen Sie es ab, um anzugeben, ob die IMM-Uhr sich automatisch anpasst, wenn die Ortszeit zwischen Standardzeit und Sommerzeit wechselt.
8. Klicken Sie auf **Save**.

Synchronisation von Taktgebern in einem Netz

Das Network Time Protocol (NTP) bietet eine Möglichkeit, Taktgeber innerhalb eines Computernetzes zu synchronisieren, wodurch jeder beliebige NTP-Client die korrekte Zeit von einem NTP-Server anfordern kann.

Die NTP-Funktion des IMM bietet eine Möglichkeit, den IMM-Taktgeber mit der Zeit zu synchronisieren, die von einem NTP-Server angegeben wird. Sie können angeben, welcher NTP-Server verwendet werden soll und wie häufig das IMM synchronisiert wird, die NTP-Funktion aktivieren oder inaktivieren und die sofortige Zeitsynchronisation anfordern.

Die NTP-Funktion bietet nicht die erweiterte Sicherheit und Authentifizierung, die in NTP Version 3 und NTP Version 4 durch Verschlüsselungsalgorithmen geboten werden. Die NTP-Funktion des IMM unterstützt nur das Simple Network Time Protocol (SNTP) ohne Authentifizierung.

Gehen Sie zum Festlegen der NTP-Funktionen des IMM wie folgt vor:

1. Melden Sie sich an dem IMM an, an dem Sie die Taktgeber des Netzes synchronisieren möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.

2. Klicken Sie im Navigationsfenster auf **System Settings** (Systemeinstellungen) und blättern Sie abwärts zum Bereich **IMM Date and Time** (IMM-Datum und -Uhrzeit).
3. Klicken Sie auf **Set IMM Date and Time** (IMM-Datum und -Uhrzeit einstellen). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

4. Unter **Network Time Protocol (NTP)** können Sie aus den folgenden Einstellungen auswählen:

   NTP auto-synchronization service
   Verwenden Sie diese Option, um die automatische Synchronisation des IMM-Taktgebers mit einem NTP-Server zu aktivieren oder zu inaktivieren.

   NTP server host name or IP address
   Geben Sie in diesem Feld den Namen des NTP-Servers an, der für die Taktgebersynchronisation verwendet werden soll.

   NTP update frequency (NTP-Aktualisierungsintervall)
   Geben Sie in diesem Feld das ungefähre Intervall (in Minuten) zwischen Synchronisationsanforderungen an. Geben Sie einen Wert zwischen 3 und 1440 Minuten ein.

   Synchronize Clock Now
   Klicken Sie auf diese Schaltfläche, um eine sofortige Synchronisation anzufordern, anstatt darauf zu warten, dass die Intervalldauer verstreicht.
5. Klicken Sie auf **Save**.

USB-Inband-Schnittstelle inaktivieren

Wichtig: Wenn Sie die USB-Inband-Schnittstelle inaktivieren, können Sie keine Inband-Aktualisierung der IMM-Firmware, der Server-Firmware und der DSA-Firmware mithilfe der Linux- oder Windows-Flashdienstprogramme durchführen. Wenn die USB-Inband-Schnittstelle inaktiviert ist, verwenden Sie die Option "Firmware Update" in der IMM-Webschnittstelle zum Aktualisieren der Firmware. Weitere Informationen hierzu finden Sie im Abschnitt „Firmware aktualisieren” auf Seite 137.

Wenn Sie die USB-Inband-Schnittstelle inaktivieren, inaktivieren Sie auch die Watchdog-Zeitlimitüberschreitungen, um zu verhindern, dass der Server unerwartet neu startet. Weitere Informationen hierzu finden Sie im Abschnitt „Serverzeitlimits festlegen” auf Seite 23.

Die USB-Inband-Schnittstelle (oder Schnittstelle "LAN over USB") wird für die Inbandkommunikation zum IMM verwendet. Um zu verhindern, dass eine Anwendung, die auf dem Server ausgeführt wird, die Ausführung von Tasks beim IMM anfordert, müssen Sie die USB-Inband-Schnittstelle inaktivieren. Weitere Informationen zu LAN over USB finden Sie in Kapitel 6, „LAN over USB”, auf Seite 143.

Gehen Sie wie folgt vor, um die USB-Inband-Schnittstelle zu inaktivieren:

1. Melden Sie sich an dem IMM an, an dem Sie die USB-Einheitentreiber-Schnittstelle inaktivieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **System Settings** (Systemeinstellungen) und blättern Sie abwärts zum Bereich **Miscellaneous** (Sonstiges). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

3. Um die USB-Inband-Schnittstelle zu inaktivieren, wählen Sie **Disabled** (Inaktiviert) in der Liste **Allow commands on the USB interface** (Befehle an der USB-Schnittstelle zulassen) aus. Die Auswahl dieser Option hat keine Auswirkungen auf die USB-Remote-Presence-Funktionen (z. B. Tastatur, Maus und Massenspeicher). Wenn Sie die USB-Inband-Schnittstelle inaktivieren, können die Inband-Systemmanagementanwendungen, wie z. B. das Dienstprogramm für erweiterte Einstellungen (ASU) und Firmware-Aktualisierungspakete möglicherweise nicht mehr verwendet werden.

   Anmerkung: Das Dienstprogramm für erweiterte Einstellungen (ASU) kann mit einer inaktivierten USB-Inband-Schnittstelle verwendet werden, wenn ein IPMI-Einheitentreiber installiert ist.
   Wenn Sie Systemmanagementanwendungen verwenden, solange die Inbandschnittstelle inaktiviert ist, funktionieren diese möglicherweise nicht.
4. Klicken Sie auf **Save** (Speichern).

Um die USB-Einheitentreiberschnittstelle zu aktivieren, nachdem sie inaktiviert wurde, heben Sie die Auswahl des Kontrollkästchens **Do not allow commands on USB interface** auf und klicken Sie dann auf **Save**.

Anmerkung:

1. Die USB-Inband-Schnittstelle wird auch als Schnittstelle "LAN over USB" bezeichnet. Sie wird in Kapitel 6, „LAN over USB”, auf Seite 143 ausführlich beschrieben.
2. Wenn Sie versuchen, eine Netzinstallation von bestimmten Linux-Distributionen zu starten, schlägt die Installation möglicherweise fehl, wenn die IMM-USB-Inband-Schnittstelle inaktiviert ist. Weitere Informationen hierzu finden Sie unter der Adresse http://rhn.redhat.com/errata/RHBA-2009-0127.html.
3. Wenn Sie eine Netzinstallation durchführen, die die Aktualisierung auf der Ret Hat-Website, die in der vorherigen Anmerkung 2 beschrieben ist, nicht enthält, müssen Sie die USB-Inband-Schnittstelle inaktivieren, bevor Sie die Installation durchführen, und nach Abschluss der Installation wieder aktivieren.
4. Informationen zur Konfiguration der Schnittstelle "LAN over USB" finden Sie im Abschnitt „Die Schnittstelle "LAN over USB" manuell konfigurieren” auf Seite 144.

Anmeldeprofil erstellen

Mithilfe der Tabelle "Login Profiles" (Anmeldeprofile) können Sie einzelne Anmeldeprofile anzeigen, konfigurieren oder ändern. Verwenden Sie die Links in der Spalte "Login ID" (Anmelde-ID), um einzelne Anmeldeprofile zu konfigurieren. Sie können bis zu 12 eindeutige Profile definieren. Jeder Link in der Spalte "Login ID" ist mit der konfigurierten Anmelde-ID und dem zugehörigen Profil gekennzeichnet.

Bestimmte Anmeldeprofile werden für die IPMI-Benutzer-IDs freigegeben und stellen eine einzige Gruppe von lokalen Benutzerkonten (Benutzername/Kennwort) bereit, die für alle IMM-Benutzerschnittstellen, einschließlich IPMI, verwendet werden können. Die Regeln, die nur diese freigegebenen Anmeldeprofile betreffen, werden in der folgenden Liste beschrieben:

- IPMI-Benutzer-ID 1 ist immer der Null-Benutzer.
- IPMI-Benutzer-ID 2 ist der Anmelde-ID 1, IPMI-Benutzer-ID 3 der Anmelde-ID 2 usw. zugeordnet.
- Für den IMM-Standardbenutzer ist `USERID` und `PASSW0RD` (mit einer Null anstelle des Buchstaben "O") für die IPMI-Benutzer-ID 2 und die Anmelde-ID 1 zugeordnet.

Beispiel: Wenn ein Benutzer durch IPMI-Befehle hinzugefügt wird, stehen diese Benutzerinformationen auch für die Authentifizierung über das Web, über Telnet, über SSH und über andere Schnittstellen zur Verfügung. Umgekehrt gilt dasselbe: wenn ein Benutzer über die Webschnittstelle oder über eine andere Schnittstelle hinzugefügt wird, stehen die betreffenden Benutzerinformationen auch zum Starten einer IPMI-Sitzung zur Verfügung.

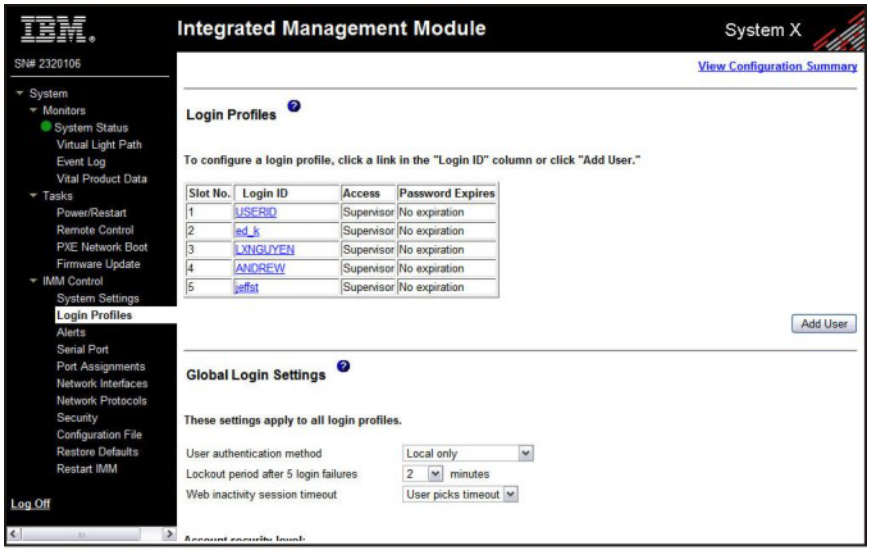
Da die Benutzerkonten gemeinsam mit IPMI verwendet werden und für diese Schnittstelle freigegeben sind, gelten bestimmte Einschränkungen, um eine gemeinsame Basis für die Schnittstellen bereitzustellen, die diese Konten verwenden. In der folgenden Liste werden die Einschränkungen für IMM- und IPMI-Anmeldeprofile beschrieben:

- Für IPMI sind maximal 64 Benutzer-IDs zulässig. Für die IPMI-Implementierung des IMM sind nur zwölf Benutzerkonten zulässig.
- Für IPMI sind anonyme Anmeldungen (Null-Benutzername und Null-Kennwort) zulässig, für das IMM jedoch nicht.
- Für IPMI sind mehrere Benutzer-IDs mit denselben Benutzernamen zulässig, für das IMM jedoch nicht.
- Auf IPMI-Anforderungen zum Ändern des Benutzernamens vom aktuellen Namen in denselben Namen wird der Fertigstellungscode `invalid parameter` (ungültiger Parameter) zurückgegeben, da der angeforderte Benutzer bereits verwendet wird.
- Die maximal IPMI-Kennwortlänge für das IMM ist 16 Byte.
- Die folgenden Begriffe sind eingeschränkt und nicht als lokale IMM-Benutzernamen verfügbar:
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

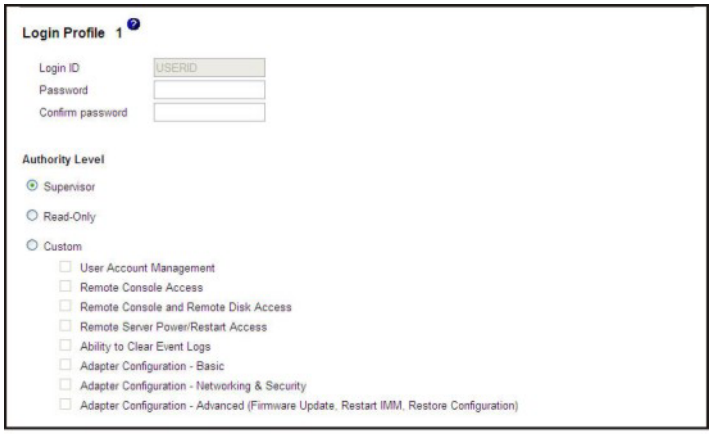
Gehen Sie wie folgt vor, um ein Anmeldeprofil zu konfigurieren:

1. Melden Sie sich an dem IMM an, auf dem Sie ein Anmeldeprofil erstellen möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Web-schnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Login Profiles** (Anmeldeprofile).

   Anmerkung: Wenn Sie kein Profil konfiguriert haben, wird es nicht in der Tabelle "Login Profiles" angezeigt.
   Auf der Seite "Login Profiles" werden alle Anmelde-IDs, die Anmeldezugriffsebenen und Informationen zum Ablauf der Kennwörter angezeigt, wie in der folgenden Abbildung dargestellt.



   Wichtig: Das IMM ist mit einem Anmeldeprofil konfiguriert, das einen Fernzugriff mit der Anmelde-Benutzer-ID `USERID` und dem Kennwort `PASSW0RD` (mit einer Null anstelle des Buchstaben "O") ermöglicht. Um ein potenzielles Sicherheitsrisiko zu vermeiden, ändern Sie dieses Standardanmeldeprofil im Verlauf der Erstkonfiguration des IMM.
3. Klicken Sie auf **Add User** (Benutzer hinzufügen). Eine Einzelprofilseite ähnlich der in der folgenden Abbildung wird angezeigt.



4. Geben Sie im Feld **Login ID** (Anmelde-ID) den Namen des Profils ein. Sie können in das Feld **Login ID** höchstens 16 Zeichen eingeben. Gültige Zeichen sind Groß- und Kleinbuchstaben, Zahlen, Punkte und Unterstreichungszeichen.

   Anmerkung: Diese Anmelde-ID wird zum Erteilen des Fernzugriffs auf das IMM verwendet.

5. Weisen Sie der Anmelde-ID im Feld **Password** (Kennwort) ein Kennwort zu. Das Kennwort muss aus mindestens fünf Zeichen bestehen, wobei ein Zeichen kein Buchstabe sein darf. Kennwörter mit einem Nullwert oder leere Kennwörter werden akzeptiert.

   Anmerkung: Dieses Kennwort wird zusammen mit der Anmelde-ID zum Erteilen des Fernzugriffs auf das IMM verwendet.

6. Geben Sie das Kennwort im Feld **Confirm password** (Kennwort bestätigen) erneut ein.

7. Wählen Sie im Bereich **Authority Level** (Berechtigungsstufe) eine der folgenden Optionen aus, um die Zugriffsberechtigung für die betreffende Anmelde-ID festzulegen:

   Supervisor (Administrator)
   Für den Benutzer gelten keine Einschränkungen.

   Read Only (Lesezugriff)
   Der Benutzer verfügt nur über Lesezugriff und kann keine Aktionen ausführen, wie z. B. Dateiübertragungen, Einschalt- und Neustartaktionen sowie Remote-Presence-Funktionen.

   Custom (Angepasst)
   Wenn Sie die Option "Custom" auswählen, müssen Sie mindestens eine der folgenden angepassten Berechtigungsstufen auswählen:

   - **User Account Management** (Benutzerkontenverwaltung): Der Benutzer andere Benutzer hinzufügen, ändern oder löschen und die globalen Anmeldungseinstellungen (unter "Global Login Settings") auf der Seite "Login Profiles" (Anmeldeprofile) ändern.
   - **Remote Console Access** (Zugriff auf die ferne Konsole): Der Benutzer kann auf die ferne Konsole zugreifen.
   - **Remote Console and Virtual Media Access** (Zugriff auf die ferne Konsole und virtuelle Datenträger): Der Benutzer kann sowohl auf die ferne Konsole als auch auf die Funktion für virtuelle Datenträger zugreifen.
   - **Remote Server Power/Restart Access** (Zugriff auf Einschalten/Neustart des fernen Servers): Der Benutzer kann auf die Einschalt- und Neustartfunktionen für den fernen Server zugreifen. Diese Funktionen sind auf der Seite "Power/Restart" verfügbar.
   - **Ability to Clear Event Logs** (Fähigkeit zum Löschen von Ereignisprotokollen): Der Benutzer kann die Ereignisprotokolle löschen. Jeder Benutzer kann die Ereignisprotokolle anzeigen. Zum Löschen der Ereignisprotokolle ist jedoch diese Berechtigung erforderlich.
   - **Adapter Configuration - Basic** (Adapterkonfiguration - Allgemein): Der Benutzer kann Konfigurationsparameter auf den Seiten "System Settings" (Systemeinstellungen) und "Alerts" ändern.
   - **Adapter Configuration - Networking & Security** (Adapterkonfiguration - Netzbetrieb & Sicherheit): Der Benutzer kann Konfigurationsparameter auf den Seiten "Security" (Sicherheit), "Network Protocols"

(Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Portzuordnungen) und "Serial Port" (Serieller Anschluss) ändern.

- **Adapter Configuration - Advanced** (Adapterkonfiguration - Erweitert): Für den Benutzer gelten keine Einschränkungen beim Konfigurieren des IMM. Zudem hat der Benutzer Verwaltungszugriff auf das IMM. Das bedeutet, dass der Benutzer auch die folgenden erweiterten Funktionen ausführen kann: Firmwareaktualisierungen, PXE-Netzboot, Wiederherstellung von werkseitigen Voreinstellungen des IMM, Ändern und Wiederherstellen der IMM-Konfiguration aus einer Konfigurationsdatei und Neustarten und Zurücksetzen des IMM.

Wenn ein Benutzer die Berechtigungsstufe einer IMM-Anmelde-ID festlegt, wird die resultierende IPMI-Berechtigungsstufe der entsprechenden IPMI-Benutzer-ID gemäß diesen Prioritäten festgelegt:

- Wenn der Benutzer als Berechtigungsstufe der IMM-Anmelde-ID "Supervisor" festlegt, wird für die IPMI-Berechtigungsstufe "Administrator" festgelegt.
- Wenn der Benutzer als Berechtigungsstufe der IMM-Anmelde-ID "Read Only" festlegt, wird für die IPMI-Berechtigungsstufe "User" festgelegt.
- Wenn der Benutzer als Berechtigungsstufe der IMM-Anmelde-ID eine der folgenden Zugriffstypen festlegt, wird für die IPMI-Berechtigungsstufe "Administrator" festgelegt:
  - User Account Management Access (Zugriff auf Benutzerkontenverwaltung)
  - Remote Console Access (Zugriff auf ferne Konsole)
  - Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)
  - Adapter Configuration - Networking & Security (Adapterkonfiguration - Netzbetrieb & Sicherheit)
  - Adapter Configuration - Advanced (Adapterkonfiguration - Erweitert)
- Wenn der Benutzer als Berechtigungsstufe der IMM-Anmelde-ID "Remote Server Power/Restart Access" oder "Ability to Clear Event Logs" festlegt, wird für die IPMI-Berechtigungsstufe "Operator" festgelegt.
- Wenn der Benutzer als Berechtigungsstufe der IMM-Anmelde-ID "Adapter Configuration (Basic)" festlegt, wird für die IPMI-Berechtigungsstufe "User" festgelegt.

Anmerkung: Um die Anmeldeprofile auf die werkseitigen Voreinstellungen zurückzusetzen, klicken Sie auf **Clear Login Profiles** (Anmeldeprofile löschen).

8. Wählen Sie im Bereich **Configure SNMPv3 User** (SNMPv3-Benutzer konfigurieren) das Kontrollkästchen aus, wenn der Benutzer mithilfe des SNMPv3-Protokolls Zugriff auf das IMM erhalten soll. Nachdem Sie das Kontrollkästchen ausgewählt haben, wird ein ähnlicher Seitenbereich wie in der folgenden Abbildung wird angezeigt.

Mit den folgenden Feldern können Sie die SNMPv3-Einstellungen für das Benutzerprofil konfigurieren:

Authentication Protocol (Authentifizierungsprotokoll)
Mithilfe dieses Felds können Sie **HMAC-MD5** oder **HMAC-SHA** als Authentifizierungsprotokoll angeben. Dabei handelt es sich um Hashalgorithmen, die vom SNMPv3-Sicherheitsmodell für die Authentifizierung verwendet werden. Das Kennwort für den Linux wird für die Authentifizierung verwendet. Wenn Sie **None** (Kein) auswählen, wird kein Authentifizierungsprotokoll verwendet.

Privacy Protocol (Datenschutzprotokoll)
Die Datenübertragung zwischen dem SNMP-Client und dem -Agenten kann mithilfe von Verschlüsselung geschützt werden. Folgende Methoden werden unterstützt: **DES** und **AES**. Die Einstellung unter "Privacy Protocol" ist nur dann gültig, wenn für das Authentifizierungsprotokoll "HMAC-MD5" oder "HMAC-SHA" festgelegt wurde.

Privacy Password (Datenschutzkennwort)
In diesem Feld können Sie das Verschlüsselungskennwort angeben.

Confirm Privacy Password (Datenschutzkennwort bestätigen)
In diesem Feld können Sie das Verschlüsselungskennwort bestätigen.

Access Type (Zugriffstyp)
Mithilfe dieses Felds können Sie **Get** (Abrufen) oder **Set** (Festlegen) als Zugriffstyp angeben. SNMPv3-Benutzer mit dem Zugriffstyp "Get" können nur Abfrageoperationen ausführen. Mit dem Zugriffstyp "Set" können SNMPv3-Benutzer Abfrageoperationen ausführen und Einstellungen ändern (z. B. das Kennwort für einen Benutzer festlegen).

Hostname/IP address for traps (Hostname/IP-Adresse für Traps)
In diesem Feld können Sie das Trapziel für den Benutzer angeben. Das kann eine IP-Adresse oder ein Hostname sein. Mithilfe von Traps benachrichtigt der SNMP-Agent die Verwaltungsstation über Ereignisse (wie z. B. wenn die Temperatur eines Prozessors den Grenzwert überschreitet).

9. Klicken Sie auf **Save** (Speichern), um Ihre Anmelde-ID-Einstellungen zu speichern.

Anmeldeprofil löschen

Gehen Sie wie folgt vor, um ein Anmeldeprofil zu löschen:

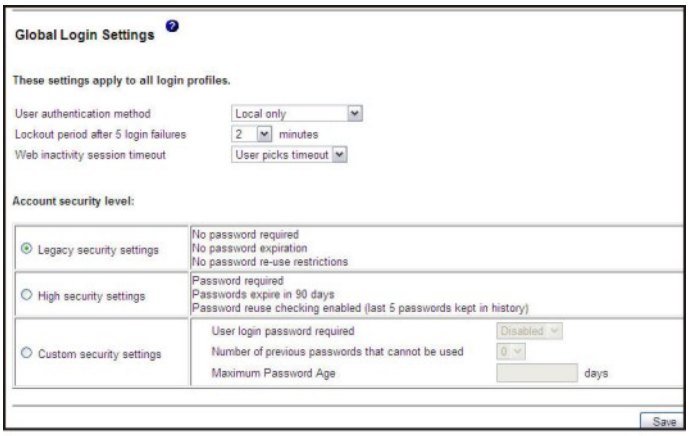
1. Melden Sie sich an dem IMM an, für das Sie ein Anmeldeprofil erstellen möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.

2. Klicken Sie im Navigationsfenster auf **Login Profiles** (Anmeldeprofile). Auf der Seite "Login Profiles" werden alle Anmelde-IDs, die Anmeldezugriffsebenen und Informationen zum Ablauf der Kennwörter angezeigt.
3. Klicken Sie auf das Anmeldeprofil, das Sie löschen möchten. Die Seite "Login Profile" für den betreffenden Benutzer wird angezeigt.
4. Klicken Sie auf **Clear Login Profile** (Anmeldeprofil löschen).

Globale Anmeldeeinstellungen konfigurieren

Gehen Sie wie folgt vor, um Bedingungen festzulegen, die für alle Anmeldeprofile für das IMM gelten:

1. Melden Sie sich an dem IMM an, für das Sie die globalen Anmeldeeinstellungen konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Login Profiles** (Anmeldeprofile).
3. Blättern Sie abwärts bis zum Bereich **Global Login Settings** (Globale Anmeldeeinstellungen). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



4. Geben Sie im Feld **User authentication method** (Benutzerauthentifizierungsmethode) an, wie die Benutzer, die versuchen, sich anzumelden, authentifiziert werden sollen. Wählen Sie eine der folgenden Authentifizierungsmethoden aus:
   - **Local only** (Nur lokal): Benutzer werden durch eine Suche in einer Tabelle authentifiziert, die lokal auf dem IMM gespeichert ist. Wenn keine Übereinstimmung für die Benutzer-ID und das Kennwort vorhanden ist, wird der Zugriff verweigert. Erfolgreich authentifizierten Benutzern wird die Berechtigungsstufe zugewiesen, die konfiguriert wurde, wie im Abschnitt „Anmeldeprofil erstellen" auf Seite 28 beschrieben.
   - **LDAP only** (Nur LDAP): Das IMM versucht, den Benutzer mithilfe des LDAP-Servers zu authentifizieren. Bei dieser Authentifizierungsmethode werden die lokalen Benutzertabellen auf dem IMM nie durchsucht.
   - **Local first, then LDAP** (Zuerst lokal, dann LDAP): Zuerst wird eine lokale Authentifizierung versucht. Falls diese lokale Authentifizierung fehlschlägt, wird eine LDAP-Authentifizierung versucht.
   - **LDAP first, then Local** (Zuerst LDAP, dann lokal): Zuerst wird die LDAP-Authentifizierung versucht. Falls diese LDAP-Authentifizierung fehlschlägt, wird eine lokale Authentifizierung versucht.

Anmerkung:

a. Nur lokal verwaltete Konten werden für die IPMI-Schnittstelle freigegeben, da IPMI die LDAP-Authentifizierung nicht unterstützt.
b. Auch wenn für das Feld **User authentication method** die Option **LDAP only** ausgewählt wird, können sich Benutzer an der IPMI-Schnittstelle anmelden, indem sie die lokal verwalteten Konten verwenden.

5. Geben Sie im Feld **Lockout period after 5 login failures** (Aussperrungszeit nach 5 Anmeldefehlern) an, wie lange (in Minuten) das IMM ferne Anmeldeversuche verhindert, wenn mehr als fünf aufeinander folgende Fehler bei der fernen Anmeldung festgestellt werden. Die Aussperrung eines Benutzers verhindert jedoch nicht die Anmeldung anderer Benutzer.
6. Geben Sie im Feld **Web inactivity session timeout** (Sitzungszeitlimit bei Webinaktivität) an, wie lange (in Minuten) das IMM wartet, bevor es die Verbindung einer inaktiven Websitzung trennt. Wählen Sie **No timeout** (Kein Zeitlimit) aus, um diese Funktion zu inaktivieren. Wählen Sie **User picks timeout** (Benutzer legt Zeitlimit fest), wenn der Benutzer das Zeitlimitintervall während des Anmeldeprozesses festlegen soll.
7. (Optional) Wählen Sie im Bereich **Account security level** (Kontensicherheitsstufe) eine Kennwortsicherheitsstufe aus. Mit den Optionen **Legacy security settings** (Traditionelle Sicherheitseinstellungen) und **High security settings** (Strenge Sicherheitseinstellungen) werden die Standardwerte festgelegt, die in der Anforderungsliste angegeben werden.
8. Um die Sicherheitseinstellungen anzupassen, wählen Sie **Custom security settings** (Angepasste Sicherheitseinstellungen) aus, um die Konfiguration des Kontensicherheitsmanagements anzuzeigen und zu ändern.
   User login password required (Kennwort für Benutzeranmeldung erforderlich)
   Geben Sie in diesem Feld an, ob eine Anmelde-ID ohne Kennwort zulässig ist.
   Number of previous passwords that cannot be used (Anzahl der vorherigen Kennwörter, die nicht verwendet werden dürfen)
   Geben Sie in diesem Feld die Anzahl der vorherigen Kennwörter an, die nicht erneut verwendet werden dürfen. Es können bis zu fünf vorherige Kennwörter verglichen werden. Wählen Sie **0** aus, um die Wiederverwendung aller vorherigen Kennwörter zuzulassen.
   Maximum Password Age (Maximale Gültigkeitsdauer des Kennworts)
   Geben Sie in diesem Feld die maximale zulässige Gültigkeitsdauer des Kennworts an, bevor das Kennwort geändert werden muss. Es werden Werte von 0 bis 365 Tagen unterstützt. Wählen Sie **0** aus, um die Überprüfung auf Ablauf der Kennwortgültigkeit zu inaktivieren.
9. Klicken Sie auf **Save** (Speichern).

Einstellungen für ferne Alerts konfigurieren

Sie können die Empfänger von fernen Alerts, die Anzahl der Alertversuche, die Vorfälle, die ferne Alerts auslösen, und lokale Alerts über den Link **Alerts** im Navigationsfenster konfigurieren.

Nachdem Sie einen Empfänger von fernen Alerts konfiguriert haben, sendet das IMM über eine Netzverbindung einen Alert an diesen Empfänger, wenn eines der Ereignisse eintritt, das in der Gruppe "Monitored Alerts" (Überwachte Alerts) ausgewählt wurde. Der Alert enthält Informationen zur Art des Ereignisses, die Uhrzeit und das Datum des Ereignisses und den Namen des Systems, das den Alert generiert hat.

Anmerkung: Wenn für die Felder **SNMP Agent** und **SNMP Traps** nicht **Enabled** (Aktiviert) festgelegt wurde, werden keine SNMP-Traps gesendet. Weitere Informationen zu diesen Feldern finden Sie im Abschnitt „SNMP (Simple Network Management Protocol) konfigurieren" auf Seite 47.

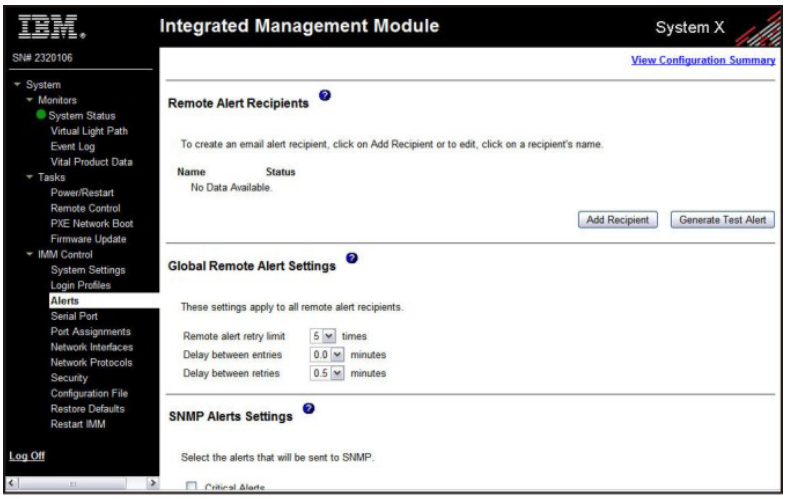
Empfänger für ferne Alerts konfigurieren

Sie können bis zu 12 eindeutige Empfänger für ferne Alerts definieren. Jeder Link für einen Alertempfänger ist mit dem Empfängernamen und dem Alertstatus gekennzeichnet.

Anmerkung: Wenn Sie noch kein Profil für Alertempfänger konfiguriert haben, wird das Profil nicht in der Liste der Empfänger der fernen Alerts angezeigt.

Gehen Sie wie folgt vor, um einen Empfänger für ferne Alerts zu konfigurieren:

1. Melden Sie sich an dem IMM an, für das Sie Einstellungen für ferne Alerts konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Alerts**. Die Seite "Remote Alert Recipients" (Empfänger für ferne Alerts) wird angezeigt. Die Benachrichtigungsmethode und der Alertstatus wird für alle Empfänger angezeigt, für die diese Einstellungen bereits festgelegt sind.



3. Klicken Sie auf einen Link für einen Empfänger für ferne Alerts oder klicken Sie auf **Add Recipient** (Empfänger hinzufügen). Ein Fenster für einen einzelnen Empfänger ähnlich dem in der folgenden Abbildung wird geöffnet.

4. Klicken Sie im Feld **Status** auf **Enabled** (Aktiviert), um den Empfänger für ferne Alerts zu aktivieren.

5. Geben Sie im Feld **Name** den Namen des Empfängers oder eine andere Kennung ein. Der Name, den Sie hier eingeben, wird auf der Seite "Alerts" als Link für den betreffenden Empfänger angezeigt.
6. Geben Sie im Feld **E-mail address** die E-Mail-Adresse des Alertempfängers ein.
7. Verwenden Sie das Kontrollkästchen, um Ereignisprotokolle in die E-Mail-Alerts einzuschließen.
8. Wählen Sie im Feld **Monitored Alerts** (Überwachte Alerts) den Alerttyp aus, der an den Alertempfänger gesendet wird. Die fernen Alerts werden nach folgenden Bewertungsstufen kategorisiert:

   Critical alerts (Kritische Alerts)
   Kritische Alerts werden für Ereignisse generiert, die signalieren, dass eine Serverkomponente nicht mehr funktioniert.

   Warning alerts (Warnalerts)
   Warnalerts werden für Ereignisse generiert, die möglicherweise einen kritischen Zustand erreichen können.

   System alerts (Systemalerts)
   Systemalerts werden für Ereignisse, die als Ergebnis von Systemfehlern auftreten, oder für Ereignisse, die als Ergebnis von Konfigurationsänderungen auftreten, generiert.

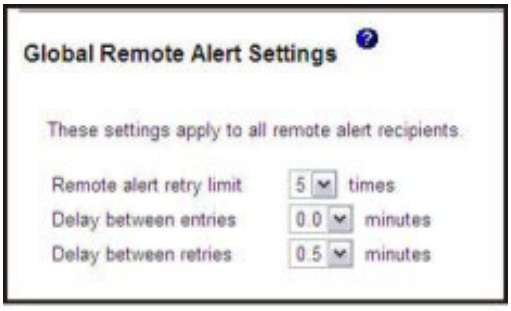
   Alle Alerts werden im Ereignisprotokoll gespeichert und an alle konfigurierten Empfänger von fernen Alerts gesendet.
9. Klicken Sie auf **Save** (Speichern).

Globale Einstellungen für ferne Alerts konfigurieren

Die globalen Einstellungen für ferne Alerts gelten nur für weitergeleitete Alerts.

Gehen Sie wie folgt vor, um die Anzahl der Versuche für das Senden eines Alerts durch das IMM festzulegen:

1. Melden Sie sich an dem IMM an, für das Sie Versuche von fernen Alerts festlegen möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Alerts** und blättern Sie abwärts zum Bereich **Global Remote Alert Settings** (Globale Einstellungen für ferne Alerts).



Verwenden Sie diese Einstellungen, um die Anzahl der Versuche für ferne Alerts und den Zeitraum zwischen diesen Versuchen zu definieren. Die Einstellungen gelten für alle konfigurierten Empfänger von fernen Alerts.

Remote alert retry limit (Wiederholungslimit für ferne Alerts)
Geben Sie im Feld **Remote alert retry limit** die Anzahl der zusätzlichen Versuche an, die das IMM unternimmt, um einen Alert an einen Empfänger zu senden. Das IMM sendet keine Mehrfachalert. Zusätzliche

Alertversuche werden nur dann ausgeführt, wenn beim ersten Sendeversuch für das Alert durch das IMM ein Fehler auftritt.

Anmerkung: Diese Alerteinstellung gilt nicht für SNMP-Alerts.

Delay between entries (Verzögerung zwischen Einträgen)
Geben Sie im Feld **Delay between entries** das Zeitintervall (in Minuten) für die Wartezeit des IMM an, bevor es einen Alert an den nächsten Empfänger in der Liste sendet.

Delay between retries (Verzögerung zwischen Wiederholungen)
Geben Sie im Feld **Delay between retries** das Zeitintervall (in Minuten) für die Wartezeit des IMM für wiederholtes Senden eines Alerts an einen Empfänger an.

3. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).

Einstellungen für SNMP-Alerts konfigurieren

Der SNMP-Agent benachrichtigt das IMM über Ereignisse durch SNMP-Traps. Sie können den SNMP-Agenten so konfigurieren, dass die Ereignisse anhand des Ereignistyps gefiltert werden. Ereigniskategorien für eine Filterung sind "Critical", "Warning" und "System". Die SNMP-Alerteinstellungen gelten global für alle SNMP-Traps.

Anmerkung:
1. Das IMM stellt zwei MIB-Dateien (Management Information Base) für SNMP-Anwendungen bereit. Die MIB-Dateien sind in den IMM-Firmwareaktualisierungspaketen enthalten.
2. Das IMM unterstützt die Standards SNMPv1 und SNMPv3.

Gehen Sie wie folgt vor, um den Alerttyp oder die Alerttypen auszuwählen, die an das SNMP gesendet werden:

1. Melden Sie sich an dem IMM an, für das Sie Versuche von fernen Alerts festlegen möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Alerts** und blättern Sie abwärts zum Bereich **SNMP Alert Settings** (Einstellungen für SNMP-Alerts).
3. Wählen Sie den Alerttyp oder die Alerttypen aus. Die fernen Alerts werden nach folgenden Bewertungsstufen kategorisiert:
   - Critical (Kritisch)
   - Warning (Warnung)
   - System
4. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).

Einstellungen für den seriellen Anschluss konfigurieren

Das IMM stellt zwei serielle Anschlüsse bereit, die für serielle Umleitungen verwendet werden.

Der serielle Anschluss 1 (COM1) auf System x Servern wird für IPMI Serial over LAN (SOL) verwendet. COM1 kann nur über die IPMI-Schnittstelle konfiguriert werden.

Auf Blade-Servern wird der serielle Anschluss 2 (COM2) für SOL verwendet. Auf System x Servern wird COM2 für serielle Umleitungen über Telnet oder SSH verwendet. COM2 kann nicht über die IPMI-Schnittstelle konfiguriert werden. Auf

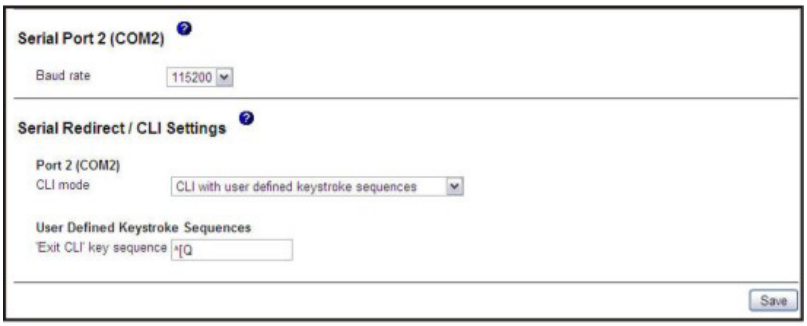
in einem Gehäuse installierten Servern und auf Turmservern ist COM2 ein interner COM-Anschluss ohne die Möglichkeit eines externen Zugriffs.

Beide serielle Anschlüsse verwenden 8 Datenbits, Parität null und 1 Stoppbit. Als Baudraten sind die Werte 9600, 19200, 38400, 57600, 115200 und 230400 möglich.

Sie können die serielle Umleitung und die Befehlszeilenschnittstelle für den Anschluss COM2 auf dem IMM konfigurieren.

Gehen Sie wie folgt vor, um die serielle Datenübertragungsgeschwindigkeit und Umleitung zu konfigurieren:

1. Melden Sie sich an dem IMM an, dessen seriellen Anschluss Sie konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Serial Port** (Serieller Anschluss). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Wählen Sie im Feld **Baud rate** (Baudrate) eine Datenübertragungsgeschwindigkeit aus, die der Geschwindigkeit des COM-Anschlusses des Servers entspricht, den Sie für die serielle Umleitung verwenden möchten. Geben Sie im Feld **Baud rate** die Datenübertragungsgeschwindigkeit Ihrer seriellen Anschlussverbindung ein. Um die Baudrate festzulegen, wählen Sie die Datenübertragungsgeschwindigkeit in Bit pro Sekunde aus, die der Geschwindigkeit Ihrer seriellen Anschlussverbindung entspricht.
4. Wählen Sie im Feld **CLI mode** (Befehlszeilenschnittstellenmodus) im Bereich **Serial Redirect/CLI Settings** (Serielle Umleitung/Einstellungen für Befehlszeilenschnittstelle) die Option **CLI with EMS compatible keystroke sequences** (Befehlszeilenschnittstelle mit EMS-kompatiblen Tastenfolgen) aus, wenn Sie eine Tastenfolge verwenden möchten, die mit Microsoft Windows Server 2003 Emergency Management Services (EMS) kompatibel ist, um die serielle Umleitungsoperation zu beenden, oder wählen Sie die Option **CLI with user defined keystroke sequences** (Befehlszeilenschnittstelle mit benutzerdefinierten Tastenfolgen) aus, wenn Sie Ihre eigene Tastenkombination verwenden möchten.

   Anmerkung: Wenn Sie die Option **CLI with user defined keystroke sequences** auswählen, müssen Sie die Tastenkombination definieren.

   Nachdem die serielle Umleitung gestartet wurde, wird sie so lange fortgesetzt, bis der Benutzer die Tastenkombination zum Beenden eingibt. Wenn die Tastenkombination zum Beenden eingegeben wird, wird die serielle Umleitung gestoppt und der Benutzer wechselt in den Befehlsmodus in der Telnet- oder SSH-Sitzung zurück. Geben Sie in diesem Feld die Tastenkombination zum Beenden an.
5. Klicken Sie auf **Save** (Speichern).

Seriell-zu-Telnet- oder SSH-Umleitung konfigurieren

Die Seriell-zu-Telnet- oder SSH-Umleitung ermöglicht es einem Systemadministrator, das IMM als seriellen Terminal-Server zu verwenden. Auf einen seriellen Serveranschluss kann ein Zugriff von eine Telnet- oder SSH-Verbindung aus erfolgen, wenn die serielle Umleitung aktiviert ist.

Anmerkungen:

1. Das IMM ermöglicht maximal zwei geöffnete Telnet-Sitzungen gleichzeitig. Über die beiden Telnet-Sitzungen kann unabhängig voneinander ein Zugriff auf die seriellen Anschlüsse erfolgen, sodass mehrere Benutzer einen umgeleiteten seriellen Anschluss gleichzeitig anzeigen können.
2. Mit dem Befehl **console 1** für die Befehlszeilenschnittstelle wird eine Sitzung für serielle Umleitung mit dem COM-Anschluss gestartet.

Beispielsitzung

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

Der gesamte Datenverkehr von COM2 wird nur zur Telnet-Sitzung umgeleitet. Der gesamte Datenverkehr von der Telnet- oder SSH-Sitzung wir zu COM2 umgeleitet.

```
ESC Q
```

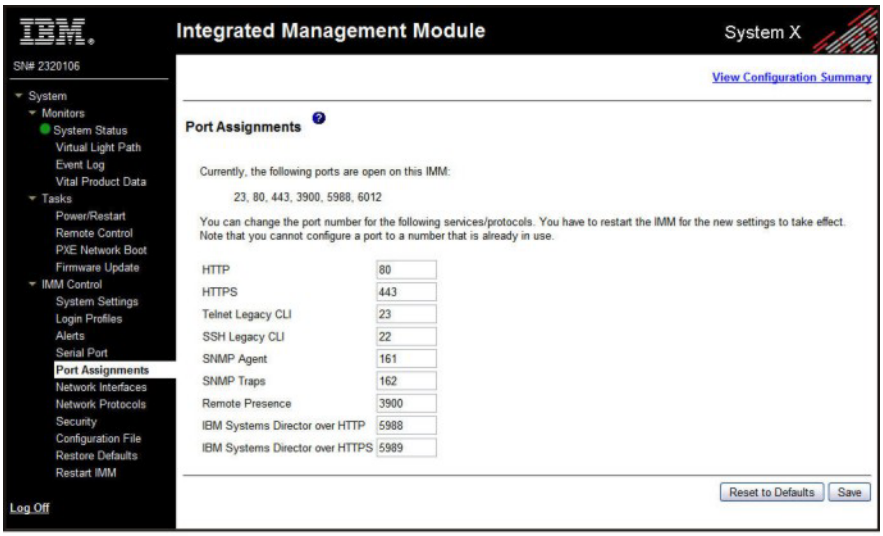
Geben Sie die Tastenkombination zum Beenden ein, um zur Befehlszeilenschnittstelle zurückzukehren. In diesem Beispiel drücken Sie die Taste "Esc" und geben dann q ein.

```
Back to LegacyCLI console....
```

Portzuordnungen konfigurieren

Gehen Sie wie folgt vor, um die Portnummern von IMM-Services zu ändern.

1. Melden Sie sich an dem IMM an, dessen Portzuordnungen Sie konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Port Assignments** (Portzuordnungen). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Verwenden Sie die folgenden Informationen, um den Feldern Werte zuzuordnen:

   HTTP Die Portnummer für den HTTP-Server des IMM. Die Standardportnummer lautet 80. Andere gültige Werte liegen im Bereich 1 - 65535. Wenn Sie diese Portnummer ändern, müssen Sie sie (mit einem Doppelpunkt vor der Nummer) an das Ende der Webadresse anhängen. Beispiel: Wenn der HTTP-Port in "8500" geändert wird, geben Sie `http://Hostname:8500/` ein, um die IMM-Webschnittstelle zu öffnen. Beachten Sie, dass Sie das Präfix `http://` vor der IP-Adresse und der Portnummer eingeben müssen.

   HTTPS
   Die Portnummer, die für Webschnittstellen-HTTPS-Datenverkehr (über SSL) verwendet wird. Der Standardwert ist 443. Andere gültige Werte liegen im Bereich 1 - 65535.

   Telnet Legacy CLI (Traditionelle Telnet-Befehlszeilenschnittstelle)
   Die Portnummer für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über den Telnet-Service. Der Standardwert ist 23. Andere gültige Werte liegen im Bereich 1 - 65535.

   SSH Legacy CLI (Traditionelle SSH-Befehlszeilenschnittstelle)
   Die Portnummer für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über SSH. Der Standardwert ist 22.

   SNMP Agent (SNMP-Agent)
   Die Portnummer für den SNMP-Agenten, der auf dem IMM ausgeführt wird. Der Standardwert ist 161. Andere gültige Werte liegen im Bereich 1 - 65535.

   SNMP Traps (SNMP-Traps)
   Die Portnummer, die für SNMP-Traps verwendet wird. Der Standardwert ist 162. Andere gültige Werte liegen im Bereich 1 - 65535.

   Remote Presence
   Die Portnummer, die die Fernsteuerungsfunktion für Anzeige und Interaktion mit der Serverkonsole verwendet. Der Standardwert lautet 3900 für in Gehäuse installierten Servern und Turmservern.

Anmerkung: Für die cKVM-Funktion (concurrent Keyboard, Video, and Mouse) von BladeCentern ist die Portnummer 2068 erforderlich. Ändern Sie diese Portnummer nicht auf einem Blade-Server.

IBM Systems Director over HTTP (IBM Systems Director über HTTP)
Die Portnummer, die IBM Systems Director für die Interaktion mit der Serverkonsole verwendet. Der Standardwert ist 5988.

IBM Systems Director over HTTPS (IBM Systems Director über HTTPS)
Die Portnummer, die IBM Systems Director für die Interaktion mit der Serverkonsole über SSL verwendet. Der Standardwert ist 5989.

Die folgenden Portnummern sind reserviert und können nur für die entsprechenden Services verwendet werden.

Tabelle 3. Reservierte Portnummern

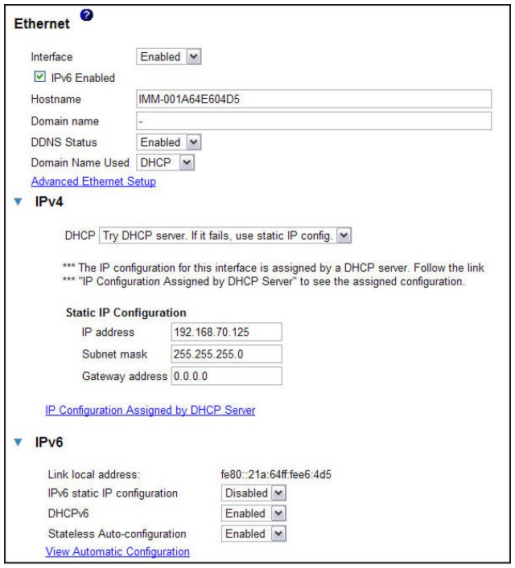
Portnummer	Für diese Services verwendet
427	SLP
7070 bis 7077	Partitionsverwaltung

4. Klicken Sie auf **Save** (Speichern).

Netzschnittstellen konfigurieren

Auf der Seite "Network Interfaces" (Netzschnittstellen) können Sie den Zugriff auf das IMM festlegen, indem Sie eine Ethernet-Verbindung zum IMM konfigurieren. Um die Ethernet-Einrichtung für das IMM zu konfigurieren, müssen Sie die Einstellungen in den Bereichen "Ethernet", "IPv4" oder "IPv6" auf der Seite "Network Interfaces" so ändern, wie es für Ihre Konfiguration erforderlich ist. Die Einstellungen dieser Bereiche werden in den folgenden Abschnitten beschrieben.

Anmerkung: Die Werte in der folgenden Abbildung sind Beispielwerte. Die Werte für Ihre Einstellungen unterscheiden sich von diesen Werten.



Um eine Zusammenfassung aller aktuellen Konfigurationseinstellungen anzuzeigen, klicken Sie auf der Seite "Network Interfaces" auf **View Configuration Summary** (Konfigurationszusammenfassung anzeigen). Bevor Sie die Einstellungen auf der Seite "Network Interfaces" konfigurieren, lesen Sie die Informationen in den folgenden Abschnitten.

Anmerkung: Sie können die IMM-Netzverbindung auch mithilfe de Konfigurationsdienstprogramms konfigurieren. Weitere Informationen hierzu finden Sie im Abschnitt „Einrichten der IMM-Netzverbindung mit dem Konfigurationsdienstprogramm der Server-Firmware für IBM System x" auf Seite 13.

Ethernet-Einstellungen konfigurieren

Die folgenden Einstellungen können im Ethernet-Bereich auf der Seite "Network Interfaces" (Netzschnittstellen) geändert werden.

Interface (Schnittstelle)
Mithilfe dieses Felds können Sie diese Netzschnittstelle aktivieren oder inaktivieren. Um Netzverbindungen über diese Netzschnittstelle zu ermöglichen, wählen Sie **Enabled** (Aktiviert) aus.

IPv6 Enabled (IPv6 aktiviert)
Mit diesem Kontrollkästchen können Sie die IPv6-Unterstützung auf dem IMM aktivieren oder inaktivieren.

Anmerkung: Wenn Sie die Auswahl des Kontrollkästchens **IPv6 Enabled** aufheben, wird das Kontrollkästchen **Hide all IPv6 configuration fields when IPv6 is disabled** (Alle IPv6-Konfigurationsfelder ausblenden, wenn IPv6 inaktiviert ist) angezeigt. Wenn Sie dieses Kontrollkästchen auswählen, wird der IPv6-Bereich auf der Seite "Network Interfaces" in der Webschnittstelle ausgeblendet.

Hostname
Mithilfe dieses Felds können Sie einen eindeutigen Hostnamen für das IMM-Subsystem definieren. Sie können in dieses Feld höchstens 63 Zeichen eingeben. Der Hostname darf nur aus alphanumerischen Zeichen, Bindestrichen und Unterstreichungszeichen bestehen.

Anmerkung: Der Hostname lautet standardmäßig `IMM-`, gefolgt von der Herstellerkennung der MAC-Adresse.

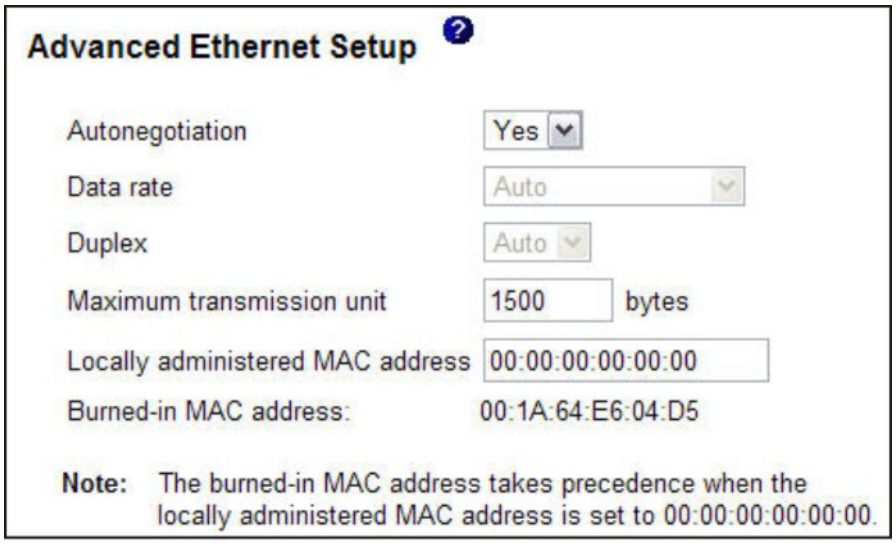
Domain name (Domänenname)
Mithilfe dieses Felds können Sie einen DNS-Domänennamen definieren.

DDNS Status
Mithilfe dieses Felds können Sie Dynamic DNS (DDNS) aktivieren oder inaktivieren. DDNS ermöglicht es dem IMM, einen DNS-Server zu benachrichtigen, um die aktive DNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderer im DNS gespeicherte Informationen in Echtzeit zu ändern. Wenn DDNS aktiviert ist, benachrichtigt IMM den DNS-Server hinsichtlich der IP-Adresse, die entweder von einem DHCP-Server oder durch Selbstkonfiguration empfangen wurde.

Domain Name Used (Verwendeter Domänenname)
Mithilfe dieses Felds können Sie auswählen, ob der DHCP-Domänenname oder der manuell zugeordnete Domänenname an den DNS gesendet wird, wenn DDNS aktiviert ist. Als Wert wird "DHCP" oder "Manual" festgelegt.

Advanced Ethernet Setup (Erweiterte Ethernet-Konfiguration)

Klicken Sie auf diesen Link, um die Seite "Advanced Ethernet Setup" zu öffnen, die der folgenden Darstellung ähnelt.



Auf dieser Seite können Sie zusätzliche Einstellungen für die Schnittstelle anzeigen und ändern. In der folgenden Tabelle werden die Einstellungen auf der Seite "Advanced Ethernet Setup" beschrieben.

Tabelle 4. Einstellungen auf der Seite "Advanced Ethernet Setup"

Einstellung	Funktion
Autonegotiation (Automatische Vereinbarung)	Mit dieser Einstellung können Sie auswählen, ob die Einstellungen für die Übertragungsgeschwindigkeit und das Duplexnetz konfigurierbar sind oder nicht. Wenn für "Autonegotiation" der Wert **Yes** (Ja) festgelegt ist, ist für die Einstellungen "Data rate" und "Duplex" der Wert **Auto** festgelegt. Diese Einstellungen sind nicht konfigurierbar. Wenn für "Autonegotiation" der Wert **No** (Nein) festgelegt ist, können Sie die Werte für die Einstellungen "Data rate" und "Duplex" konfigurieren.
Data rate (Übertragungsgeschwindigkeit)	Mithilfe dieses Felds können Sie das Datenvolumen angeben, das pro Sekunde über Ihre LAN-Verbindung übertragen werden kann. Um die Übertragungsgeschwindigkeit festzulegen, wählen Sie die Datenübertragungsgeschwindigkeit in Megabit (Mb) aus, die der Funktionalität Ihres Netzes entspricht. Wählen Sie **Auto** aus, wenn die Datenübertragungsgeschwindigkeit automatisch erkannt werden soll.

Tabelle 4. Einstellungen auf der Seite "Advanced Ethernet Setup" (Forts.)

Einstellung	Funktion
Duplex	Mithilfe dieses Feldes können Sie den Kommunikationskanaltyp angeben, der in Ihrem Netz verwendet wird. Um den Duplexmodus festzulegen, wählen Sie entweder **Full** (Vollduplex) oder **Half** (Halbduplex) aus. Mit Vollduplex können die Daten in beide Richtungen gleichzeitig übertragen werden. Ein Halbduplexkanal ermöglicht das Übertragen von Daten in die eine oder in die andere Richtung, aber nicht in beide Richtungen gleichzeitig. Wählen Sie **Auto** aus, wenn der Duplextyp automatisch erkannt werden soll.
Maximum transmission unit (MTU) (Größte zu übertragende Einheit)	Mithilfe dieses Feldes können Sie die maximale Größe eines Datenpakets (in Byte) für Ihre Netzschnittstelle angeben. Um den Wert für die MTU festzulegen, geben Sie die gewünschte Zahl in das Textfeld ein. Für Ethernet ist der gültige MTU-Bereich 68 bis 1.500.
Locally administered MAC address (Lokal verwaltete MAC-Adresse)	Mithilfe dieses Feldes können Sie eine physische Adresse für dieses IMM-Subsystem angeben. Wenn ein Wert angegeben wird, setzt die lokal verwaltete Adresse die Herstellerkennung der MAC-Adresse außer Kraft. Die lokal verwaltete Adresse muss ein Hexadezimalwert zwischen 000000000000 und FFFFFFFFFFFF sein. Dieser Wert muss im Format *XX:XX:XX:XX:XX:XX* angegeben werden, wobei *X* für eine Zahl von 0 bis 9 und einen Buchstaben von A bis F steht. Die Verwendung einer Multicastadresse ist für das IMM nicht zulässig. Bei einer Multicastadresse hat das niedrigstwertige Bit des ersten Byte den Wert 1. Aus diesem Grund muss das erste Byte eine gerade Zahl sein.
Burned-in MAC address (Herstellerkennung der MAC-Adresse)	Die Herstellerkennung der MAC-Adresse ist eine eindeutige physische Adresse, die dem IMM vom Hersteller zugeordnet wurde.

IPv4-Einstellungen konfigurieren

Die folgenden Einstellungen können im IPv4-Bereich auf der Seite "Network Interfaces" (Netzschnittstellen) geändert werden.

DHCP Mithilfe dieses Felds können Sie angeben, ob die TCP/IP-Einstellungen des Ethernet-Anschlusses des IMM-Subsystems durch einen DHCP-Server (Dynamic Host Configuration Protocol) in Ihrem Netz festgelegt werden sollen. Um die DHCP-Konfiguration zu verwenden, wählen Sie **Enabled: Obtain IP config. from DHCP server** (Aktiviert: IP-Konfiguration vom DHCP-Server beziehen) aus. Um Ihre TCP/IP-Einstellungen manuell zu konfigurieren, wählen Sie **Disabled - Use static IP configuration** (Inaktiviert: Statische IP-Konfiguration verwenden) aus. Wenn Sie versuchen möchten, einen DHCP-Server zu verwenden, und anschließend zur stati-

schen IP-Konfiguration zurückkehren möchten, wenn kein DHCP-Server erreicht werden kann, wählen Sie **Try DHCP server. If it fails, use static IP config** (Nach DHCP-Server suchen. Falls das fehlschlägt, statische IP-Konfiguration verwenden) aus.

Wenn die IP-Konfiguration durch einen DHCP-Server zugeordnet wird, klicken Sie auf den Link **IP Configuration Assigned by DHCP server** (Durch DHCP-Server zugeordnete IP-Konfiguration), um die Konfigurationsdetails anzuzeigen.

Anmerkung:

1. Wenn Sie die Option **Enabled - Obtain IP config. from DHCP server** auswählen, muss ein zugänglicher, aktiver konfigurierter DHCP-Server in Ihren Netz vorhanden sein.
2. Die Konfiguration, die durch einen DHCP-Server zugeordnet wird, setzt alle statischen IP-Einstellungen außer Kraft.
3. Die Option **Try DHCP server. If it fails, use static IP config.** wird nicht auf allen IMMs unterstützt.

Static IP Configuration (Statische IP-Konfiguration)

Die folgenden Felder enthalten die statische IP-Konfiguration für diese Schnittstelle. Diese Einstellungen werden nur dann verwendet, wenn DHCP inaktiviert ist. Wenn DHCP aktiviert ist, setzt die dynamische IP-Konfiguration, die durch den DHCP-Server zugeordnet wird, diese statischen Einstellungen außer Kraft.

- **IP address** (IP-Adresse): Mithilfe dieses Felds können Sie die IP-Adresse des IMM definieren, auf das ein Zugriff über diese Netzschnittstelle erfolgt. Geben Sie die Adresse in das Textfeld ein, um die IP-Adresse festzulegen. Die IP-Adresse muss vier Ganzzahlen (von 0 bis 255) enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen enthalten.

  Anmerkung: Der Standardwert für dieses Feld lautet `192.168.70.125`.
- **Subnet mask** (Teilnetzmaske): Mithilfe dieses Felds können Sie die Teilnetzmaske definieren, die vom IMM-Subsystem verwendet wird. Um die Teilnetzmaske festzulegen, geben Sie die Bitmaske in das Textfeld ein. Die Teilnetzmaske muss vier Ganzzahlen (von 0 bis 255) enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen enthalten. Die in Kontingenten festgelegten Bits beginnen mit dem Bit ganz links. Beispiel: `0.255.0.0` ist keine gültige Teilnetzmaske. Dieses Feld kann nicht mit `0.0.0.0` oder `255.255.255.255` festgelegt werden.

  Anmerkung: Der Standardwert für dieses Feld lautet `255.255.255.0`.
- **Gateway address** (Gateway-Adresse): Mithilfe dieses Felds können Sie die IP-Adresse Ihres Standard-Gateways angeben. Geben Sie die Adresse in das Textfeld ein, um die Gateway-Adresse festzulegen. Die Gateway-Adresse muss vier Ganzzahlen (von 0 bis 255) enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen oder aufeinanderfolgende Punkte enthalten.

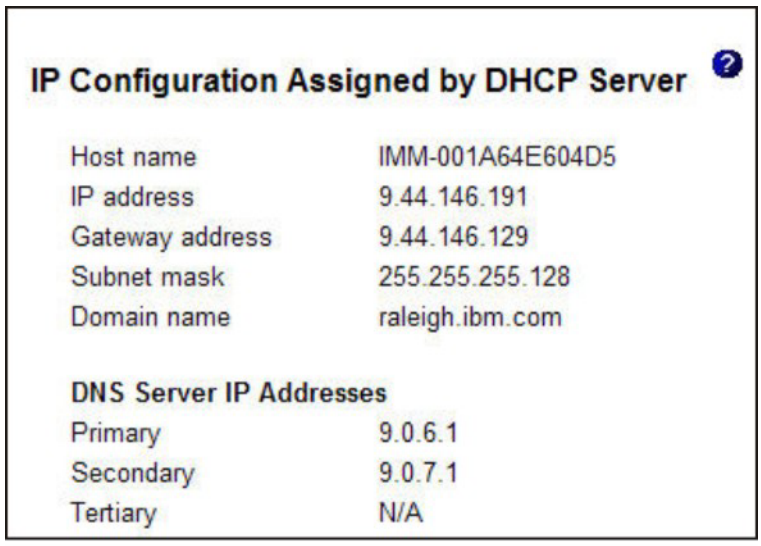
  Anmerkung: Der Standardwert für dieses Feld lautet `0.0.0.0`.

IP Configuration Assigned by DHCP Server (Durch DHCP-Server zugeordnete IP-Konfiguration)

Klicken Sie auf diesen Link, um die vom DHCP-Server zugeordnete IP-

Konfiguration anzuzeigen. Die Seite "IP Configuration Assigned by DHCP Server" (ähnlich der folgenden Darstellung) wird angezeigt.

Anmerkung: Diese Option ist nur verfügbar, wenn DHCP aktiviert ist.



IPv6-Einstellungen konfigurieren

Die folgenden Einstellungen können im IPv6-Bereich auf der Seite "Network Interfaces" (Netzschnittstellen) geändert werden.

Anmerkung: Mindestens eine der IPv6-Konfigurationsoptionen, die in diesem Abschnitt beschrieben werden (IPv6 Static Configuration, DHCPv6 oder Stateless Auto-configuration) muss aktiviert sein.

Link local address (Lokale Verbindungsadresse)
Die lokale Verbindungsadresse ist die IPv6-Adresse, die dem IMM zugeordnet ist. Die lokale Verbindungsadresse wird in einem Format angegeben, das dem im folgenden Beispiel ähnelt:

```
fe80::21a:64ff:fee6:4d5
```

IPv6 Static Configuration (Statische VPv6-Konfiguration)
Mithilfe dieses Felds können Sie die statischen Konfigurationseinstellungen für IPv6 aktivieren oder inaktivieren. Wenn das Kontrollkästchen **IPv6 Static Configuration** ausgewählt wird, sind die folgenden Optionen verfügbar:

- **IP address** (IP-Adresse): Mithilfe dieses Felds können Sie die IPv6-Adresse des IMM definieren, auf das ein Zugriff über diese Netzschnittstelle erfolgt. Geben Sie die IPv6-Adresse in das Textfeld ein, um die IP-Adresse festzulegen. Der Wert in diesem Feld muss eine gültige IPv6-Adresse sein.

  Anmerkung: Der Standardwert für dieses Feld lautet `0::0`.
- **Address prefix length (1 - 128)** (Länge des Adressenpräfix): Mithilfe dieses Felds können Sie die Präfixlänge für die statische IPv6-Adresse festlegen.

- **Default route** (Standardroute): Mithilfe dieses Felds können Sie die IPv6-Adresse Ihrer Standardroute festlegen. Geben Sie die IPv6-Adresse in das entsprechende Feld ein, um die Standardroute festzulegen. Der Wert in diesem Feld muss eine gültige IPv6-Adresse sein.

  Anmerkung: Der Standardwert für dieses Feld lautet `0::0`.

DHCPv6
Mithilfe dieses Felds können Sie die zugeordnete DHCPv6-Konfiguration auf dem IMM aktivieren oder inaktivieren.

Stateless Auto-configuration (Statusunabhängige automatische Konfiguration)
Mithilfe dieses Felds können Sie die statusunabhängige automatische Konfiguration auf dem IMM aktivieren oder inaktivieren.

View Automatic Configuration (Link) (Automatische Konfiguration anzeigen)
Um die IPv6-Konfiguration anzuzeigen, die durch den DHCP-Server zugeordnet wurden, klicken Sie auf diesen Link. Die Seite "IPv6 Automatic Configuration" wird angezeigt.

Netzprotokolle konfigurieren

Auf der Seite "Network Protocols" können Sie die folgenden Funktionen ausführen:

- SNMP (Simple Network Management Protocol) konfigurieren
- DNS (Domain Name System) konfigurieren
- Telnet-Protokoll konfigurieren
- SMTP (Simple Mail Transfer Protocol) konfigurieren
- LDAP (Lightweight Directory Access Protocol) konfigurieren
- SLP (Service Location Protocol) konfigurieren

Änderungen an den Einstellungen des Netzprotokolls erfordern, dass das IMM erneut gestartet wird, damit die Änderungen wirksam werden. Wenn Sie mehrere Protokolle ändern, können Sie warten, bis alle Protokolländerungen abgeschlossen und gespeichert sind, bevor Sie das IMM erneut starten.

SNMP (Simple Network Management Protocol) konfigurieren

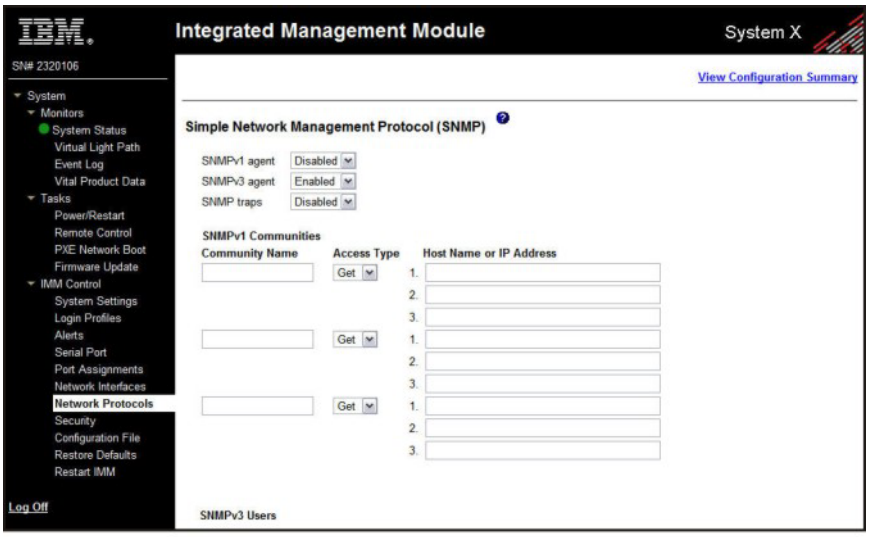
Sie können den SNMP-Agenten zum Erfassen von Informationen und zum Steuern des Servers verwenden. Das IMM kann auch zum Senden von SNMP-Alerts an die konfigurierten Hostnamen oder IP-Adressen konfiguriert werden.

Anmerkung:

1. Das IMM stellt zwei MIB-Dateien (Management Information Base) für SNMP-Anwendungen bereit. Die MIB-Dateien sind in den IMM-Firmwareaktualisierungspaketen enthalten.
2. Das IMM unterstützt die Standards SNMPv1 und SNMPv3.

Gehen Sie wie folgt vor, um SNMP zu konfigurieren:

1. Melden Sie sich an dem IMM an, dessen SNMP Sie konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Wählen Sie **Enabled** (Aktiviert) im Feld für **SNMPv1 agent** oder im Feld für **SNMPv3 agent** aus.

   Anmerkung: Wenn Sie den SNMPv3-Agenten aktivieren, müssen Sie anschließend die SNMPv3-Einstellungen für aktive Anmeldeprofile so konfigurieren, dass die Interaktion zwischen dem SNMPv3-Manager und dem SNMPv3-Agenten ordnungsgemäß abläuft. Sie können diese Einstellungen unten in den Einstellungen für die einzelnen Anmeldeprofile auf der Seite "Login Profiles" (Anmeldeprofile) konfigurieren (weitere Informationen hierzu finden Sie im Abschnitt „Anmeldeprofil erstellen” auf Seite 28). Klicken Sie auf den Link des Anmeldeprofils, das Sie konfigurieren möchten, blättern Sie auf der Seite nach unten und klicken Sie dann auf das Kontrollkästchen **Configure SNMPv3 User** (SNMPv3-Benutzer konfigurieren).
4. Wählen Sie im Feld **SNMP traps** (SNMP-Traps) die Option **Enabled** (Aktiviert) aus, um Alerts an die SNMP-Communitys in Ihrem Netz weiterzuleiten. Folgende Kriterien müssen erfüllt sein, um einen SNMP-Agenten aktivieren zu können:
   - Auf der Seite "System Settings" (Systemeinstellungen) muss ein Systemansprechpartner angegeben sein. Informationen zu den Einstellungen auf der Seite "System Settings" finden Sie im Abschnitt „Einstellung von Systeminformationen” auf Seite 22.
   - Auf der Seite "System Settings" muss eine Systemadresse angegeben sein.
   - Es muss mindestens ein Community-Name angegeben sein.
   - Für diese Community muss mindestens eine gültige IP-Adresse oder ein gültiger Hostname (wenn DNS aktiviert ist) angegeben sein.

   Anmerkung: Alertempfänger mit der Benachrichtigungsmethode SNMP erhalten Alerts nur, wenn für das Feld **SNMPv1 agent** oder das Feld **SNMPv3 agent** und für das Feld **SNMP traps** die Einstellung **Enabled** festgelegt ist.
5. Konfigurieren Sie eine Community, um die Verwaltungsbeziehung zwischen SNMP-Agenten und SNMP-Managern zu definieren. Sie müssen mindestens eine Community definieren. Jede Community-Definition enthält folgende Parameter:

- Community Name (Community-Name)
- Access Type (Zugriffstyp)
- IP address (IP-Adresse)

Wenn einer dieser Parameter nicht korrekt ist, wird der SNMP-Managementzugriff nicht erteilt werden.

Anmerkung: Wenn ein Fenster mit einer Fehlernachricht angezeigt wird, nehmen Sie in den Feldern, die im Fehlerfenster aufgeführt sind, die notwendigen Korrekturen vor. Blättern Sie anschließend zum Seitenende und klicken Sie auf **Save** (Speichern), um die korrigierten Daten zu speichern. Sie müssen mindestens eine Community konfigurieren, um diesen SNMP-Agenten zu aktivieren.

6. Geben Sie im Feld **Community Name** (Community-Name) einen Namen oder eine Zeichenfolge zur Authentifizierung ein, um die Community zu benennen.
7. Wählen Sie im Feld **Access Type** (Zugriffstyp) einen Zugriffstyp aus. Wählen Sie **Trap** aus, um allen Hosts in der Community den Empfang von Traps zu ermöglichen. Wählen Sie **Get** aus, um allen Hosts in der Community den Empfang von Traps und die Abfrage von MIB-Objekten zu ermöglichen. Wählen Sie **Set** aus, allen Hosts in der Community den Empfang von Traps, die Abfrage von MIB-Objekten und das Festlegen von MIB-Objekten zu ermöglichen.
8. Geben Sie im entsprechenden Feld **Host Name** (Hostname) oder **IP Address** (IP-Adresse) den Hostnamen oder die IP-Adresse der einzelnen Community-Manager ein.
9. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
10. Klicken Sie im Navigationsfenster auf **Restart IMM** (IMM erneut starten), um die Änderungen zu aktivieren.

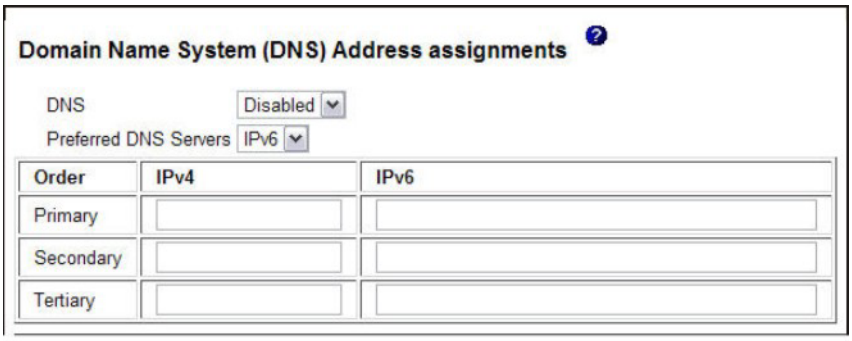
DNS konfigurieren

Sie können die DNS-Einstellungen (Domain Name System) konfigurieren und dabei angeben, ob zusätzliche DNS-Serveradressen in die Suchreihenfolge für die Auflösung von Hostnamen zu IP-Adressen einbezogen werden sollen. Die DNS-Suche ist immer aktiviert. Andere DNS-Adressen werden möglicherweise automatisch vom DHCP-Server zugeordnet, wenn die DHCP-Funktionalität aktiviert ist.

Damit die zusätzlichen DNS-Adressen aktiviert werden, muss mindestens eine dieser Adressen einen anderen Wert als null aufweisen. Die zusätzlichen DNS-Server werden an den Anfang der Suchliste hinzugefügt, sodass die Hostnamensuche auf diesen Servern ausgeführt wird, bevor sie auf einem DNS-Server ausgeführt wird, der automatisch durch einen DHCP-Server zugeordnet wird.

Gehen Sie wie folgt vor, um DNS zu konfigurieren:

1. Melden Sie sich an dem IMM an, dessen DNS Sie konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle) und blättern Sie auf der Seite abwärts bis zum Bereich **Domain Name System (DNS) Address assignments** (DNS-Adresszuordnungen). Ein ähnlicher Seitenabschnitt wie in der folgenden Abbildung wird angezeigt.



3. Wenn mindestens ein DNS-Server in Ihrem Netz zur Verfügung steht, wählen Sie im Feld **DNS** die Option **Enabled** (Aktiviert) aus. Das Feld **DNS** gibt an, ob Sie in Ihrem Netz einen DNS-Server verwenden, um Hostnamen in IP-Adressen zu übersetzen.
4. Wenn Sie IPv4- und IPv6-DNS-Serveradressen verwenden, wählen Sie entweder **IPv4** oder **IPv6** in der Liste **Preferred DNS Servers** (Bevorzugte DNS-Server) aus, um anzugeben, welche Serveradressen Sie bevorzugt verwenden möchten.
5. Wenn Sie DNS aktiviert haben, verwenden Sie die Textfelder "Primary", "Secondary" und "Tertiary", um die IP-Adressen von bis zu sechs DNS-Servern in Ihrem Netz anzugeben. Um drei IPv4- oder drei IPv6-DNS-Serveradressen anzugeben, geben Sie die Adressen in die entsprechenden Textfelder ein. Stellen Sie sicher, dass die IPv4- oder IPv6-Adressen in einem gültigen Format angegeben sind.
6. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
7. Klicken Sie im Navigationsfenster auf **Restart IMM** (IMM erneut starten), um die Änderungen zu aktivieren.

Telnet konfigurieren

Gehen Sie wie folgt vor, um Telnet zu konfigurieren:

1. Melden Sie sich an dem IMM an, dessen Telnet Sie konfigurieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle) und blättern Sie auf der Seite abwärts bis zum Bereich **Telnet Protocol** (Telnet-Protokoll). Sie können die maximale Anzahl an gleichzeitigen Telnet-Benutzern festlegen oder den Telnet-Zugriff inaktivieren.
3. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
4. Klicken Sie im Navigationsfenster auf **Restart IMM** (IMM erneut starten), um die Änderungen zu aktivieren.

SMTP (Simple Mail Transfer Protocol) konfigurieren

Gehen Sie wie folgt vor, um die IP-Adresse oder den Hostnamen des SMTP-Servers (Simple Mail Transfer Protocol) anzugeben.

1. Melden Sie sich an dem IMM an, dessen SMTP Sie konfigurieren möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle) und blättern Sie auf der Seite abwärts bis zum Bereich **SMTP**.

3. Geben Sie im Feld **SMTP Server Host Name or IP address** (Hostname oder IP-Adresse des SMTP-Servers) den Hostnamen des SMTP-Servers ein. Geben Sie in diesem Feld die IP-Adresse oder, wenn DNS aktiviert und konfiguriert ist, den Hostnamen des SMTP-Servers ein.
4. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
5. Klicken Sie im Navigationsfenster auf **Restart IMM** (IMM erneut starten), um die Änderungen zu aktivieren.

LDAP konfigurieren

Mithilfe eines LDAP-Servers (Lightweight Directory Access Protocol) kann das IMM einen Benutzer durch Abfragen oder Durchsuchen eines LDAP-Verzeichnisses auf einem LDAP-Server ohne Abfragen der lokalen Benutzerdatenbank authentifizieren. Anschließend kann das IMM jeden Benutzerzugriff über einen zentralen LDAP-Server authentifizieren. Dafür ist LDAP-Clientunterstützung auf dem IMM erforderlich. Sie können außerdem Berechtigungsstufen auf der Basis der Informationen auf dem LDAP-Server zuordnen.

Sie können LDAP auch dazu verwenden, Benutzer und IMMs Gruppen zuzuordnen und eine Gruppenauthentifizierung zusätzlich zu der normalen Benutzerauthentifizierung (Kennwortprüfung) durchzuführen. Ein IMM kann z. B. einer oder mehreren Gruppen zugehörig sein. In diesem Fall besteht ein Benutzer die Gruppenauthentifizierung nur dann, wenn er zu mindestens einer der Gruppen gehört, die dem IMM zugeordnet sind.

Dieser Abschnitt enthält Informationen zur Konfiguration der folgenden beiden LDAP-Server:

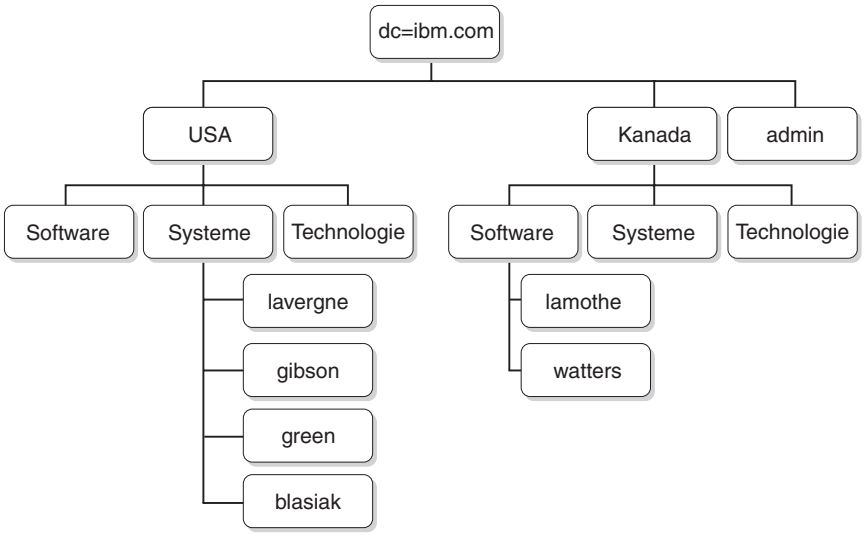
- Novell eDirectory Version 8.7.1
- Microsoft Windows Server 2003 Active Directory

Beispiel für ein Benutzerschema

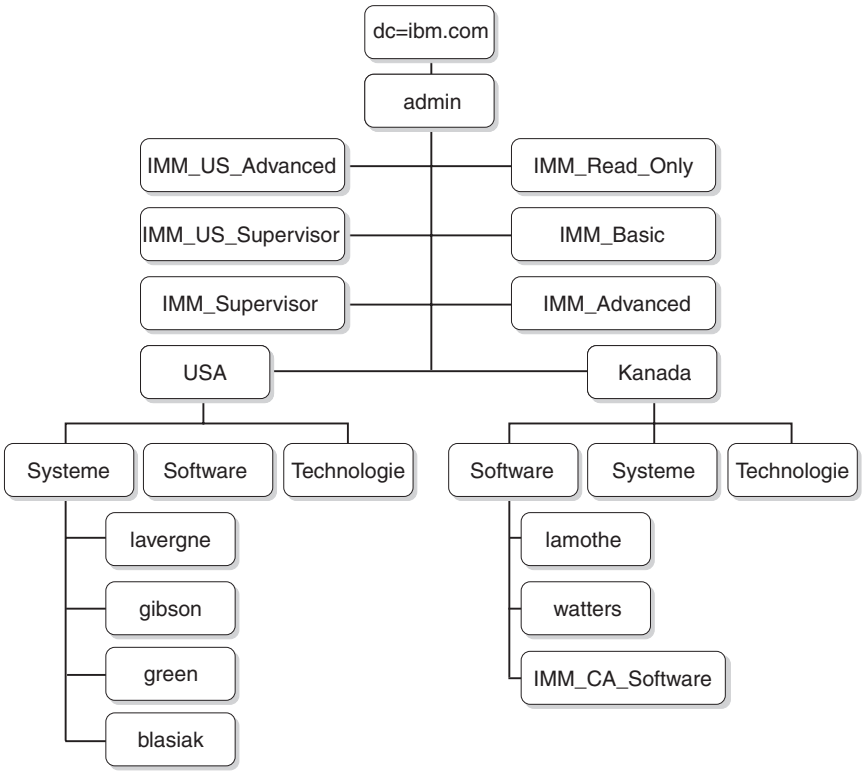
In diesem Abschnitt wird ein Beispiel für ein einfaches Benutzerschema beschrieben. Dieses Schemabeispiel wird im ganzen Dokument wiederholt für die Darstellung der Konfiguration des LDAP-Clients und des LDAP-Server verwendet.

Das Benutzerschemabeispiel weist als Stammelement eine Domänenkomponente mit dem Namen "ibm.com" auf. Dies bedeutet, dass bei allen Objekten in dieser Verzeichnisstruktur der definierte Name für den Stammeintrag "dc=ibm,dc=com" lautet. Nehmen Sie an, dass diese Verzeichnisstruktur ein Unternehmen darstellt, das Benutzer und Benutzergruppen anhand von Ländern und Organisationen klassifizieren möchte. Die Hierarchie lautet "Stammelement → Land → Organisation → Personen".

In der folgenden Abbildung ist eine vereinfachte Ansicht des Schemas, das in diesem Dokument verwendet wird, dargestellt. Beachten Sie, dass ein Benutzerkonto (userid=admin) unmittelbar unter dem Stammelement verwendet wird. Dieser Benutzer ist der Administrator.



In der folgenden Abbildung ist das Hinzufügen von Benutzergruppen dargestellt. Es werden sechs Benutzergruppen definiert und zur ersten Ebene hinzugefügt; eine weitere Benutzergruppe wird zur Organisation "Software" im Land "Canada" hinzugefügt.



Die Benutzer und die zugehörigen Benutzergruppen in Tabelle 5 werden zur Vervollständigung des Schemas verwendet.

Tabelle 5. Zuordnung des Benutzers zu einer Gruppe

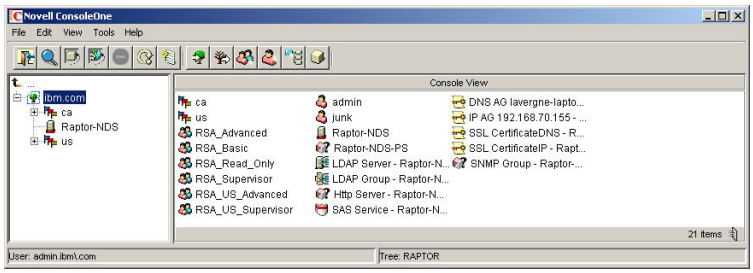
Definierter Name des Benutzers	**Gruppenzugehörigkeit**
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com

Tabelle 5. Zuordnung des Benutzers zu einer Gruppe (Forts.)

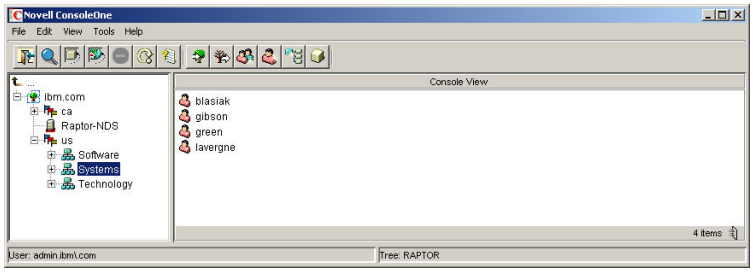
Definierter Name des Benutzers	Gruppenzugehörigkeit
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Novell eDirectory-Schemaansicht

Mithilfe des Novell ConsoleOne-Tools wurde das Schema, das im Abschnitt „Beispiel für ein Benutzerschema” auf Seite 51 beschrieben wird, in ein Novell eDirectory extrahiert. In der folgenden Abbildung ist die oberste Ebene des Schemas dargestellt, wie sie im ConsoleOne-Tool angezeigt wird.



In der folgenden Abbildung werden die Benutzer unter o=Systems, c=us, dc=ibm.com erfasst.



Gruppenzugehörigkeit

Novell eDirectory verwendet das Attribut **GroupMembership** (Gruppenzugehörigkeit), um die Gruppen zu identifizieren, zu denen ein Benutzer gehört. Insbesondere die Objektklasse "User" verwendet dieses Attribut. Der LDAP-Client verwendet in der Suchanforderung an den LDAP-Server den Standardwert **memberOf**, wenn die Gruppen abgefragt werden, bei denen ein Benutzer ein Mitglied ist (bzw. zu denen ein Benutzer gehört).

Sie können den LDAP-Client für Zugehörigkeitsabfragen mit einer der folgenden Methoden konfigurieren:

- Konfigurieren Sie den Wert **GroupMembership** im Feld **Group Search Attribute** (Gruppensuchattribut) auf dem LDAP-Client.
- Erstellen Sie eine Attributzuordnung zwischen **GroupMembership** und **memberOf** auf dem Novell eDirectory-LDAP-Server.

Gehen Sie wie folgt vor, um das Standardattribut auf dem LDAP-Client zu konfigurieren:

1. Klicken Sie im linken Navigationsfenster in der IMM-Webschnittstelle auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie bis zum Bereich **LDAP Search Attributes** (LDAP-Suchattribute).
3. Geben Sie im Feld **Group Search Attribute** das gewünschte Standardattribut ein.

Wenn das Feld **Group Search Attribute** leer ist, wird der Standardwert **memberOf** verwendet. In diesem Fall müssen Sie den Novell eDirectory-Server für die Zuordnung des Attributs **GroupMembership** zu **memberOf** konfigurieren. Gehen Sie wie folgt vor, um den Novell eDirectory-Server für die Zuordnung des Attributs **GroupMembership** zu **memberOf** zu konfigurieren.

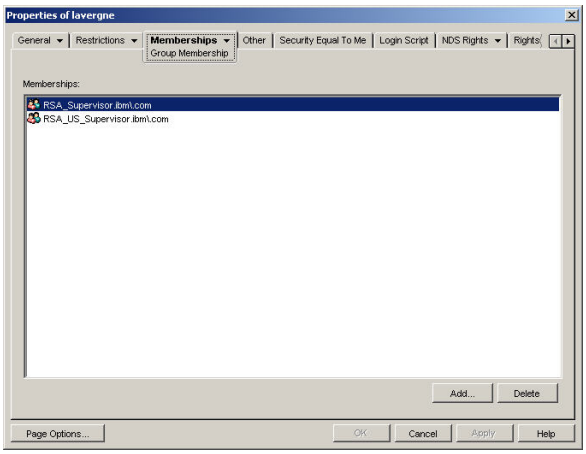
1. Klicken Sie im ConsoleOne-Tool mit der rechten Maustaste auf das Symbol **LDAP Group** (LDAP-Gruppe) und klicken Sie anschließend auf **Properties** (Eigenschaften). Das Fenster "Properties of LDAP Group" wird geöffnet.
2. Klicken Sie auf die Registerkarte **Attribute Mappings** (Attributzuordnungen).
3. Klicken Sie auf **Add** (Hinzufügen) und erstellen Sie eine Zuordnung zwischen **Group Membership** und **memberOf**.
4. Klicken Sie auf **OK**. Eine Seite, in der die Eigenschaften der LDAP-Gruppe angezeigt werden, wird geöffnet.

Benutzer zu Benutzergruppen hinzufügen

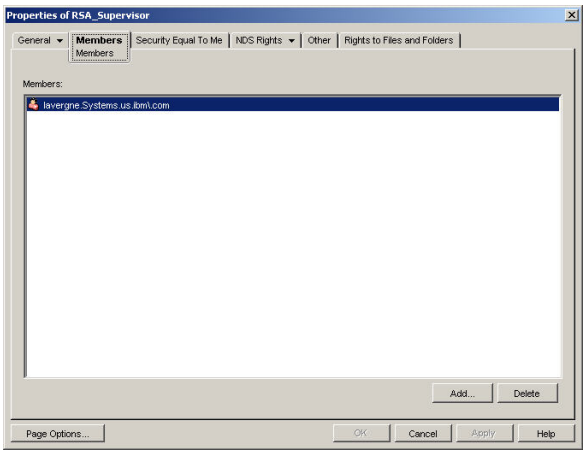
Sie können Benutzer den entsprechenden Benutzergruppen hinzufügen, indem Sie entweder Gruppen dem Profil eines Benutzers hinzufügen oder indem Sie einen Benutzer zum Profil einer Gruppe hinzufügen. Das Endergebnis ist dasselbe.

Im vorherigen Benutzerschemabeispiel etwa ist Benutzer lavergne Mitglied sowohl von IMM_US_Supervisor als auch von IMM_Supervisor. Mithilfe eines Browsertools wie etwa Novell ConsoleOne können Sie das Schema bestätigen (klicken Sie zweimal auf **user lavergne** und wählen Sie die Registerkarte **Memberships (Mitgliedschaften)**.

Eine Seite ähnlich der in der folgenden Abbildung wird geöffnet.



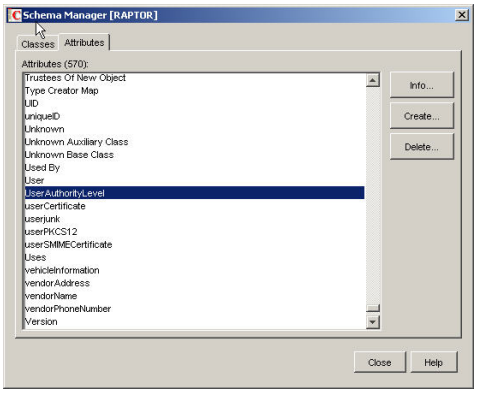
Desgleichen gilt: Wenn die Eigenschaften der Gruppe IMM_Supervisor angezeigt werden und Sie die Registerkarte **Members** (Mitglieder) auswählen, wird eine Seite ähnlich der in der folgenden Abbildung geöffnet.



Berechtigungsstufen

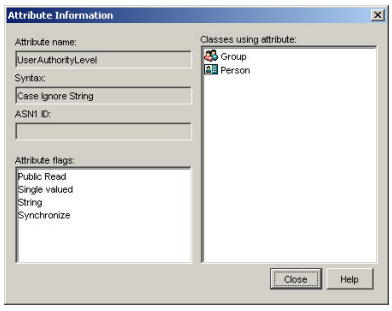
Zum Verwenden der Berechtigungsstufenfunktion erstellen Sie mit ConsoleOne ein neues Attribut mit dem Namen `UserAuthorityLevel` auf dem Novell eDirectory. Dieses neue Attribut wird zur Unterstützung von Berechtigungsstufen verwendet.

1. Klicken Sie im Tool Novell ConsoleOne auf **Tools** > **Schema Manager**.
2. Klicken Sie auf die Registerkarte **Attributes** und dann auf **Create** (Erstellen).
3. Bezeichnen Sie das Attribut als **UserAuthorityLevel**. Lassen Sie **ASN1 ID** leer oder wenden Sie sich an Ihren Administrator, um festzustellen, welcher Wert verwendet werden soll. Klicken Sie auf **Next**.
4. Setzen Sie die Syntax auf **Case Ignore String** (Zeichenfolge, bei der die Groß-/Kleinschreibung ignoriert wird). Klicken Sie auf **Next**.
5. Setzen Sie die Flags auf "applicable" (zutreffend). Wenden Sie sich an Ihren LDAP-Administrator, um sicherzustellen, dass diese richtig eingestellt sind. Klicken Sie auf das Kontrollkästchen **Public Read** (Öffentlich lesbar); klicken Sie dann auf **Next**.
6. Klicken Sie auf **Finish** (Fertigstellen). Eine Seite ähnlich der in der folgenden Abbildung wird geöffnet.



7. Kehren Sie zum Fenster "Schema Manager" zurück und klicken Sie auf die Registerkarte **Classes**.
8. Klicken Sie auf die Klasse **Person** und dann auf **Add** (Hinzufügen). Beachten Sie, dass Sie stattdessen auch die Klasse "User object" (Benutzerobjekt) verwenden können.
9. Blättern Sie abwärts zum Attribut **UserAuthorityLevel**, wählen Sie es aus und fügen Sie es zu den Attributen für diese Klasse hinzu. Klicken Sie auf **OK**.

10. Klicken Sie auf die Klasse **Group** (Gruppe) und dann auf **Add**.
11. Blättern Sie abwärts zum Attribut **UserAuthorityLevel**, wählen Sie es aus und fügen Sie es zu den Attributen für diese Klasse hinzu. Klicken Sie auf **OK**.
12. Um zu bestätigen, dass das Attribut erfolgreich zur Klasse hinzugefügt wurde, wählen Sie im Fenster "Schema Manager" die Klasse **Attributes**.
13. Blättern Sie zum Attribut **UserAuthorityLevel** und klicken Sie dann auf **Info**. Eine Seite ähnlich der in der folgenden Abbildung wird geöffnet.



Berechtigungsstufen einrichten

In diesem Abschnitt wird erklärt, wie das Attribut "UserAuthorityLevel" zu verstehen und zu verwenden ist. Der Wert, der dem Attribut "UserAuthorityLevel" zugewiesen wird, bestimmt, welche Berechtigungen (oder Berechtigungsstufen) einem Benutzer nach erfolgreicher Authentifizierung zugewiesen werden.

Das Attribut "UserAuthorityLevel" wird als Bitfolge, also als Folge von Nullen und Einsern, gelesen. Die Bits werden von links nach rechts gezählt. Das erste Bit ist Bitposition 0, das zweite Bit ist Bitposition 1 und so weiter.

In der folgenden Tabelle wird jede Bitposition erklärt.

Tabelle 6. Berechtigungsbits

Bit- position	**Funktion**	**Erläuterung**
0	Deny Always (Nie zulassen)	Wenn dieses Bit gesetzt ist, wird die Authentifizierung eines Benutzers immer fehlschlagen. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
1	Supervisor Access (Administratorzugriff)	Wenn dieses Bit gesetzt ist, wird einem Benutzer die Administratorberechtigung erteilt. Der Benutzer hat Schreib-/Lesezugriff auf jede Funktion. Wenn Sie dieses Bit einstellen, müssen Sie die anderen Bits nicht einzeln einstellen.

Tabelle 6. Berechtigungsbits (Forts.)

Bit- position	Funktion	Erläuterung
2	Read Only Access (Schreibgeschützter Zugriff)	Wenn dieses Bit gesetzt ist, hat ein Benutzer schreibgeschützten Zugriff und kann keine Wartungsarbeiten durchführen (beispielsweise Neustart, fern ausgeführte Aktionen oder Firmwareaktualisierungen). Nichts kann durch Speicher-, Lösch- oder Wiederherstellungsfunktionen geändert werden. Bitposition 2 und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung hat. Wenn irgendein anderes Bit eingestellt ist, wird dieses Bit ignoriert.
3	Networking (Netzbetrieb) & Security	Wenn dieses Bit gesetzt ist, kann ein Benutzer die Konfiguration in den Anzeigen "Security", "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Anschlusszuordnungen) und "Serial Port" (Serieller Anschluss) ändern.
4	User Account Management (Benutzerkontenverwaltung)	Wenn dieses Bit gesetzt ist, kann ein Benutzer andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) in der Anzeige "Login Profiles" (Anmeldeprofile) ändern.
5	Remote Console Access (Zugriff auf ferne Konsole)	Wenn dieses Bit gesetzt ist, hat ein Benutzer Zugriff auf die Remote-Server-Konsole und kann die Konfiguration in der Anzeige "Serial Port" ändern.
6	Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)	Wenn dieses Bit gesetzt ist, kann ein Benutzer auf die Remote-Server-Konsole und die fernen Datenträgerfunktionen für den fernen Server zugreifen. Der Benutzer kann außerdem die Konfiguration in der Anzeige "Serial Port" ändern.
7	Remote Server Power/Restart Access (Zugriff auf Einschalten/Neustart des fernen Servers)	Wenn dieses Bit gesetzt ist, kann ein Benutzer auf die Einschalt-, Neustart- und Serverzeitlimitfunktionen für den fernen Server zugreifen.
8	Basic Adapter Configuration (Basisadapterkonfiguration)	Wenn dieses Bit gesetzt ist, kann ein Benutzer Konfigurationsparameter in den Anzeigen "System Settings" (Systemeinstellungen) und "Alerts" ändern (ausgenommen die Parameter "Contact", "Location" und "Server Timeout" (Serverzeitlimit)).

Tabelle 6. Berechtigungsbits (Forts.)

Bit- position	Funktion	Erläuterung
9	Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)	Wenn dieses Bit gesetzt ist, kann ein Benutzer die Ereignisprotokolle löschen. **Anmerkung:** Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu können, muss der Benutzer diese Berechtigungsstufe haben.
10	Advanced Adapter Configuration (Erweiterte Adapterkonfiguration)	Wenn dieses Bit gesetzt ist, ist ein Benutzer beim Konfigurieren des Adapters nicht eingeschränkt und hat Verwaltungszugriff auf das IMM. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE-Netzboot, werkseitige Adaptervoreinstellungen wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wiederherstellen und den Adapter erneut starten bzw. zurücksetzen. Hiervon ausgenommen sind die Funktion "Server Power/Restart Control" (Steuerung von Einschalten/Neustart des Servers) und die Zeitlimitfunktion.
11	Reserved (Reserviert)	Diese Bitposition ist für den künftigen Gebrauch reserviert (zurzeit nicht relevant).

Anmerkungen:

- Wenn Bits nicht verwendet werden, wird der Standard für den Benutzer auf "Read Only" (Schreibgeschützt) eingestellt.
- Priorität haben die Anmeldeberechtigungen, die direkt aus dem Benutzersatz abgerufen werden. Wenn der Benutzersatz im Feld **Login Permission Attribute** (Anmeldeberechtigungsattribut) keinen Namen enthält, wird versucht, die Berechtigungen von den Gruppen abzurufen, denen der Benutzer angehört und die mit dem Gruppenfilter übereinstimmen. In diesem Fall wird dem Benutzer das inklusive ODER aller Bits für alle Gruppen zugewiesen.
- Wenn das Bit für "Deny Always" (Bitposition null) für irgendeine der Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit "Deny Always" hat vor allen anderen Bits Vorrang.
- Wenn ein Benutzer die Fähigkeit hat, allgemeine sowie Netzbetriebs- oder Sicherheits-Adapterkonfigurationsparameter zu ändern, sollten Sie erwägen, diesem Benutzer die Fähigkeit zu geben, das IMM erneut zu starten (Bitposition zehn). Ohne diese Fähigkeit kann ein Benutzer zwar möglicherweise einen Parameter ändern, dieser Parameter wird jedoch nicht wirksam.

In der folgenden Tabelle stehen Beispiele und ihre Beschreibungen:

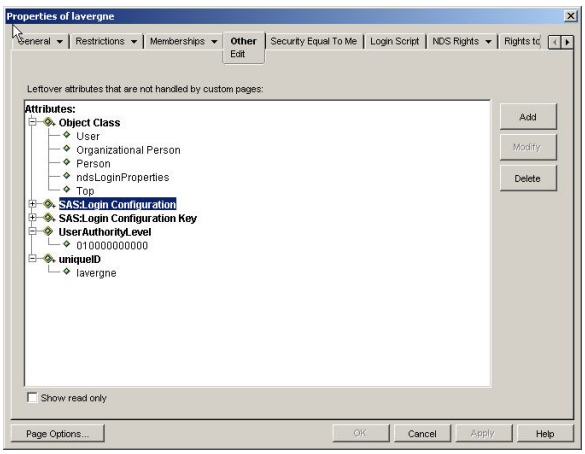
Tabelle 7. Beispiel "UserLevelAuthority"-Attribute und Beschreibungen

Beispiel UserLevelAuthority-Attribut	Beschreibung
IBMRBSPermissions=010000000000	"Supervisor Access" (Bitposition 1 ist gesetzt)
IBMRBSPermissions=001000000000	"Read-Only Access" (Bitposition 2 ist gesetzt)
IBMRBSPermissions=100000000000	"No Access" (Kein Zugriff) (Bitposition 0 ist gesetzt)
IBMRBSPermissions=000011111100	Alle Berechtigungen außer "Advanced Adapter Configuration"
IBMRBSPermissions=000011011110	Alle Berechtigungen außer Zugang zu virtuellem Datenträger

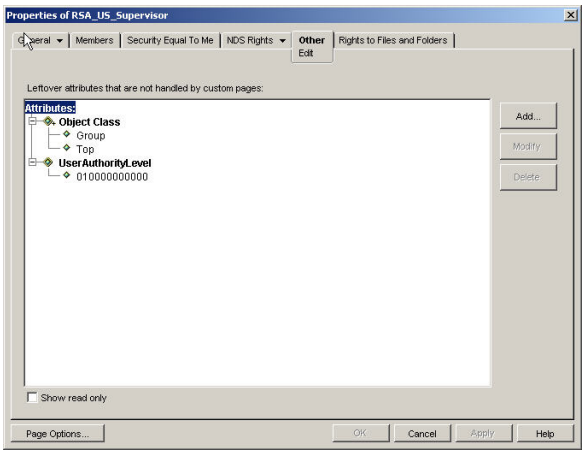
Gehen Sie wie folgt vor, um zu Benutzer *lavergne* und zu jeder der Benutzergruppen das Attribut "UserAuthorityLevel" hinzuzufügen:

1. Klicken Sie mit der rechten Maustaste auf den Benutzer **lavergne** und klicken Sie auf **Properties (Eigenschaften)**.
2. Klicken Sie auf die Registerkarte **Other** (Andere). Klicken Sie auf **Add** (Hinzufügen).
3. Blättern Sie abwärts auf **UserAuthorityAttribute** und klicken Sie auf **OK**.
4. Geben Sie den Wert ein, den das Attribut haben soll. Wenn Sie beispielsweise den Administratorzugriff zuweisen möchten, setzen Sie das Attribut auf **IBMRBSPermissions=010000000000**. Klicken Sie auf **OK**.
5. Wiederholen Sie die Schritte 1 bis 4 für jede Benutzergruppe und legen Sie die Stufe **UserAuthorityLevel** als geeignet fest.

   In der folgenden Abbildung sind die Eigenschaften von Benutzer *lavergne* dargestellt.



In der folgenden Abbildung sind die Eigenschaften von IMM_US_Supervisor dargestellt.



In der folgenden Tabelle steht die **UserAuthorityLevel**, die jeder der Benutzergruppen im Benutzerschemabeispiel jeweils zugewiesen ist.

Tabelle 8. "UserAuthorityLevel"-Zuweisungen an Benutzergruppen

Benutzergruppe	UserAuthorityLevel	Übersetzung
IMM_Basic	IBMRBSPermissions=000100000000	Netzbetrieb und Sicherheit
IMM_CA_Software	IBMRBSPermissions=000101111010	Netzbetrieb und Sicherheit Zugriff auf ferne Konsole und virtuellen Datenträger Zugriff auf Stromversorgung und Neustart des fernen Servers Allgemeine Adapterkonfiguration Erweiterte Adapterkonfiguration
IMM_Advanced	IBMRBSPermissions=000110111100	Netzbetrieb und Sicherheit Zugriff auf ferne Konsole und virtuellen Datenträger Zugriff auf Stromversorgung und Neustart des fernen Servers Allgemeine Adapterkonfiguration Erweiterte Adapterkonfiguration Fähigkeit, Ereignisprotokolle zu löschen
IMM_Supervisor	IBMRBSPermissions=010000000000	Administratorzugriff
IMM_Read_Only	IBMRBSPermissions=001000000000	Schreibgeschützter Zugriff

Tabelle 8. "UserAuthorityLevel"-Zuweisungen an Benutzergruppen (Forts.)

Benutzergruppe	UserAuthorityLevel	Übersetzung
IMM_US_Advanced	IBMRBSPermissions=000110111100	Netzbetrieb und Sicherheit Benutzerkontenverwaltung Zugriff auf ferne Konsole und virtuellen Datenträger Zugriff auf Stromversorgung und Neustart des fernen Servers Allgemeine Adapterkonfiguration Fähigkeit, Ereignisprotokolle zu löschen
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Administratorzugriff

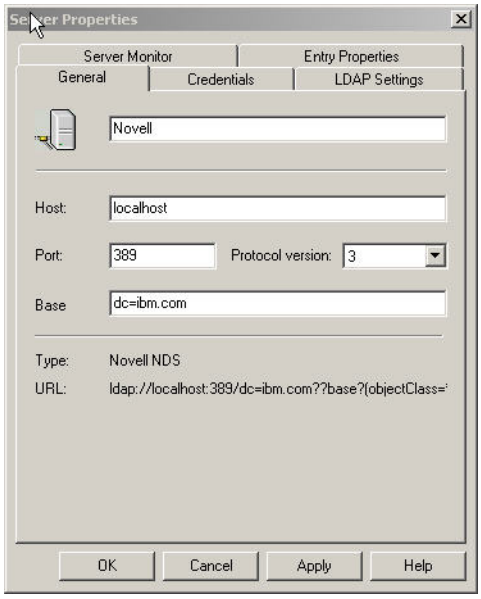
LDAP-Server durchsuchen

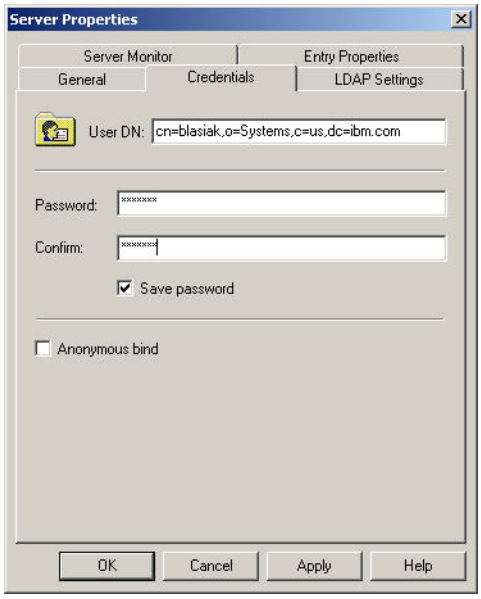
Bevor Sie versuchen, eine Verbindung vom LDAP-Client auf dem IMM eine Verbindung zu Ihrem LDAP-Server herzustellen, stellen Sie zuerst mithilfe eines LDAP-Browsers eines anderen Herstellers eine Verbindung zum LDAP-Server her. Beispiel: Unter der Adresse http://www.ldapbrowser.com finden Sie ein entsprechendes Verzeichnis-Browser-Tool.

Die Verwendung eines LDAP-Browsers vor dem Versuch, den IMM-LDAP-Client zu verwenden, hat die folgenden Vorteile:

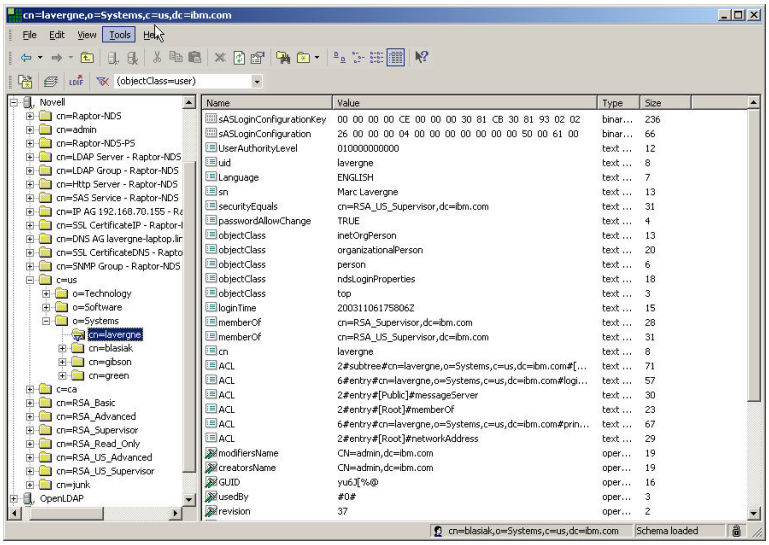
- Sie haben die Möglichkeit, eine Bindung mit verschiedenen Berechtigungsnachweisen zu einem Server zu erstellen. Dadurch können Sie testen, ob die Benutzerkonten auf dem LDAP-Server ordnungsgemäß konfiguriert sind. Wenn Sie mit dem Browser eine Bindung zum Server erstellen können, dieser Vorgang jedoch mit dem IMM-LDAP-Client fehlschlägt, ist der LDAP-Client falsch konfiguriert. Wenn Sie keine Bindung mit dem Browser erstellen können, werden Sie auch keine Bindung mit dem LDAP-Client auf dem IMM erstellen können.
- Nachdem Sie erfolgreich eine Bindung an den Server erstellt haben, können Sie in der LDAP-Serverdatenbank navigieren und schnelle Suchanfragen ausgeben. Dadurch können Sie überprüfen, ob der LDAP-Server so konfiguriert ist, wie Sie es für den Zugriff auf die verschiedenen Objekte geplant haben. Beispiel: Sie können überprüfen, ob Sie ein bestimmtes Attribut anzeigen können oder ob alle erwarteten Objekte auf eine bestimmte Suchanforderung angezeigt werden. Ist dies nicht der Fall, kann es bedeuten, dass die Berechtigungen, die den Objekten zugeordnet wurden (z. B., welche Objekte öffentlich sichtbar und welche verdeckt sind), nicht richtig konfiguriert wurden. Wenden Sie sich an den LDAP-Serveradministrator, um den Fehler zu beheben. Beachten Sie, dass der Berechtigungsnachweis, den Sie für die Bindung verwenden, bestimmt, welche Zugriffsrechte Sie auf dem Server haben.
- Überprüfen Sie die Gruppenzugehörigkeit für alle Benutzer. Überprüfen Sie das Attribut **UserAuthorityLevel**, das Benutzern und Benutzergruppen zugeordnet ist.

In den folgenden Abbildungen sind verschiedene Abfragen und Suchergebnisse dargestellt, die an einen Novell eDirectory-Server gesendet wurden, der gemäß den Anweisungen im Abschnitt „Beispiel für ein Benutzerschema” auf Seite 51 konfiguriert wurde. In diesem Fall wurde das Softerra LDAP-Browser-Tool verwendet. Die einleitende Bindung zum Server wurde mit den Eigenschaften und Berechtigungsnachweisen erstellt, die in der Abbildung dargestellt sind.

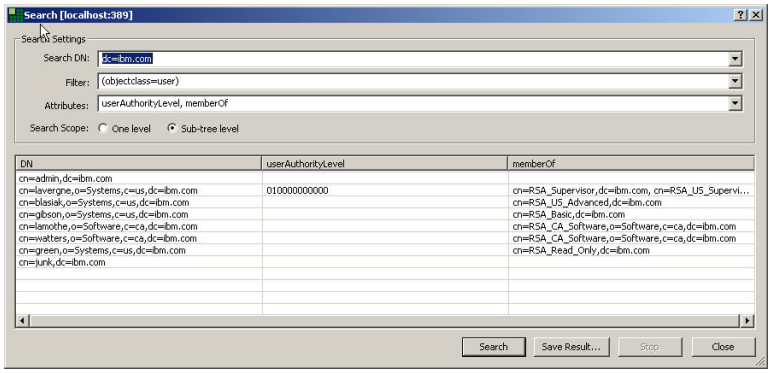




Nachdem die einleitende Bindung erfolgreich war, erscheint die folgende Ansicht eines Schemas in Novell eDirectory.



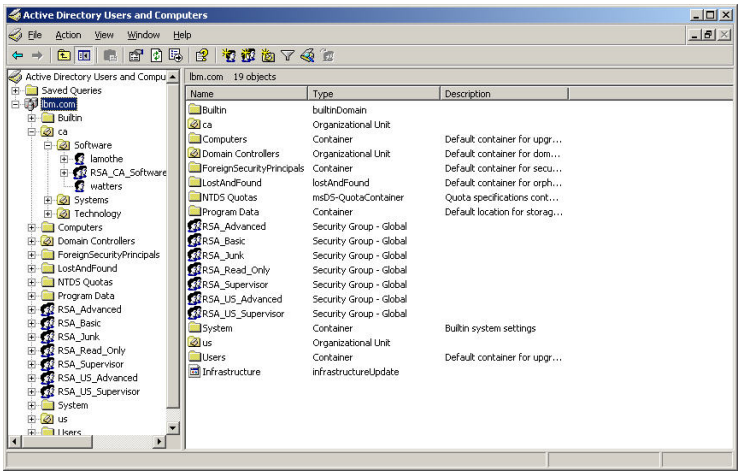
In der folgenden Abbildung ist eine Abfrage aller Benutzer mit der Anforderung, die Attribute **userAuthorityLevel** und **memberOf** abzurufen, dargestellt.



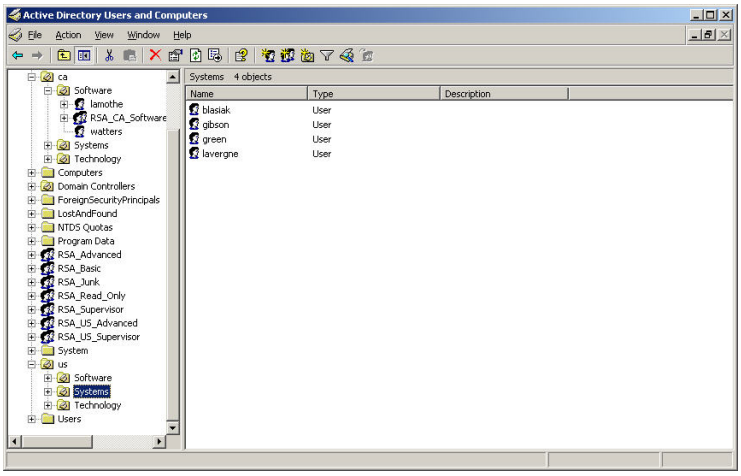
Schemaansicht von Microsoft Windows Server 2003 Active Directory

In diesem Abschnitt werden einige der Konfigurationsaspekte beschrieben, die in Beziehung zum Erfassen der Informationen im Abschnitt „Beispiel für ein Benutzerschema” auf Seite 51 mit Microsoft Windows Server 2003 Active Directory stehen.

In der folgenden Abbildung ist die oberste Ebene des Schemas dargestellt, wie sie im Verwaltungstool "Active Directory-Benutzer und -Computer" angezeigt wird.



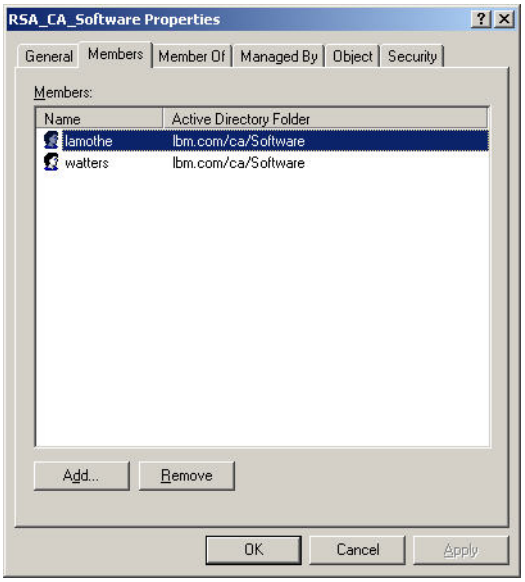
In der folgenden Abbildung sind die Benutzer unter ou=Systems, ou=us, dc=ibm, dc=com dargestellt.



Benutzer zu Benutzergruppen hinzufügen

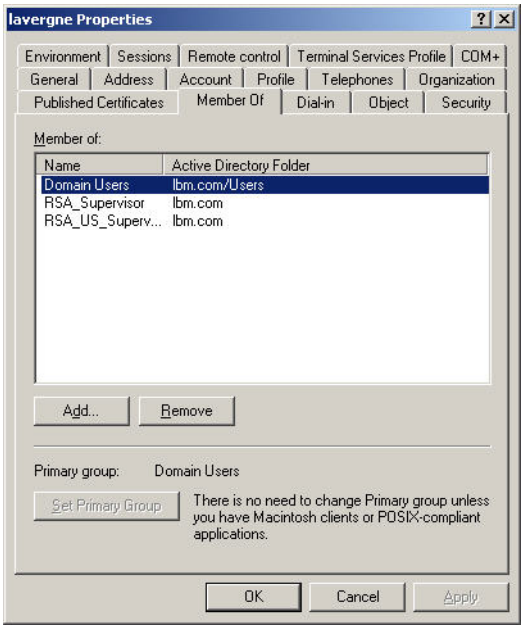
In Active Directory können Sie entweder Gruppen zu einem bestimmten Benutzer oder Benutzer zu einer bestimmten Gruppe hinzufügen. Klicken Sie mit der rechten Maustaste auf das Benutzer- oder das Benutzergruppenobjekt und wählen Sie **Properties** (Eigenschaften) aus.

Wenn Sie eine Benutzergruppe auswählen und anschließend auf die Registerkarte **Members** (Mitglieder) klicken, wird eine Seite ähnlich der in der folgenden Abbildung geöffnet.



Um Benutzer zur Benutzergruppe hinzuzufügen oder aus ihr zu löschen, klicken Sie auf **Add** (Hinzufügen) oder auf **Remove** (Entfernen).

Wenn Sie einen Benutzer auswählen und anschließend auf die Registerkarte **MembersOf** (Mitglied von) klicken, wird eine Seite ähnlich der in der folgenden Abbildung geöffnet.

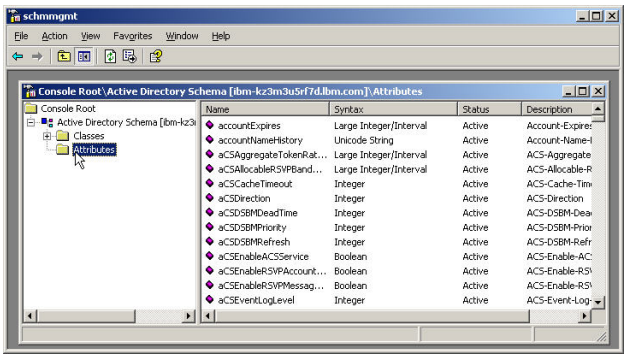


Um Benutzer zur Benutzergruppe hinzuzufügen oder aus ihr zu löschen, klicken Sie auf **Add** (Hinzufügen) oder auf **Remove** (Entfernen).

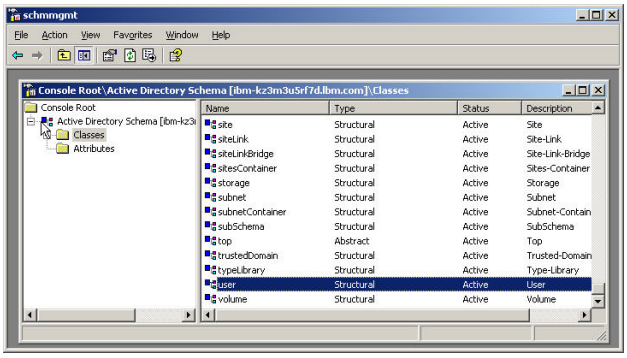
Berechtigungsstufen

Im Abschnitt „Berechtigungsstufen” auf Seite 55 ist beschrieben, wie Sie mit dem Novell eDirectory-Server ein neues Attribut zum Unterstützen des Konzepts von Berechtigungsstufen erstellen und wie diese Berechtigungsstufen Benutzern zugeordnet werden, die sich von einem IMM aus an einem LDAP-Server authentifizieren. Das neu erstellte Attribut wurde **UserAuthorityLevel** genannt. In diesem Abschnitt werden Sie dieses Attribut auf Active Directory erstellen.

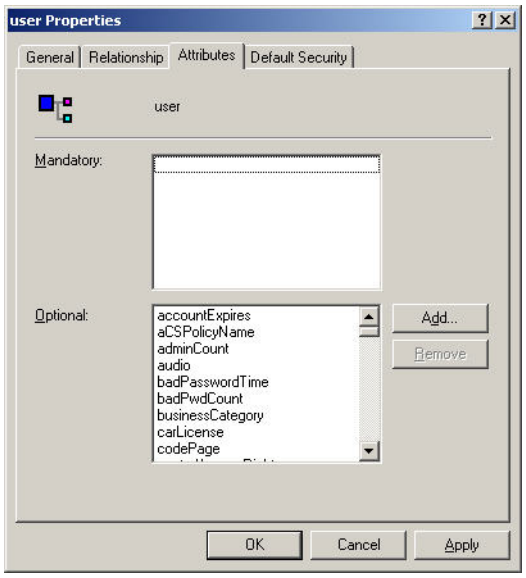
1. Installieren Sie das Snap-in-Tool des Active Directory-Schema. Weitere Informationen finden Sie in der Dokumentation zu Active Directory.
2. Starten Sie das Active Directory-Schema.
3. Klicken Sie auf **Action** > **Create Attribute (Attribut erstellen)**. Machen Sie in folgenden Feldern die erforderlichen Angaben:
   a. Setzen Sie "Common Name" (Allgemeiner Name) auf **UserAuthorityLevel**
   b. Setzen Sie "Syntax" auf **Case Insensitive String** (Zeichenfolge, bei der die Groß-/Kleinschreibung nicht berücksichtigt werden muss)
   c. Setzen Sie "Minimum" und "Maximum" auf **12**
4. Wenden Sie sich an Ihren Systemadministrator, um eine neue X.500-Verfasser-ID zuzuweisen. Wenn Sie keine neue X.500-Verfasser-ID definieren möchten, verwenden Sie ein bestehendes Attribut, anstatt ein neues Attribut für die Berechtigungsstufe zu erstellen.



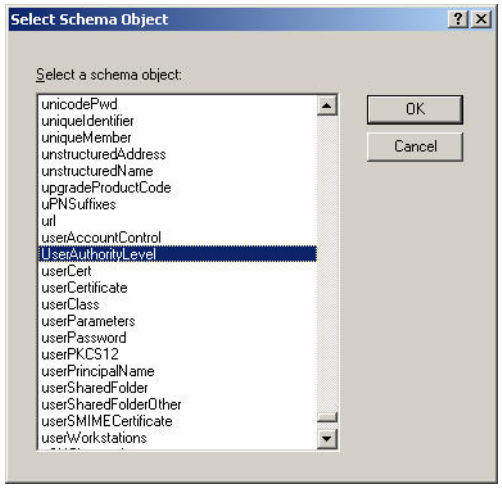
5. Nachdem das Attribut gespeichert ist wählen Sie den Ordner **Classes**.



6. Klicken Sie zweimal auf die Klasse **user** (Benutzer). Das Fenster mit den Benutzereigenschaften wird geöffnet.

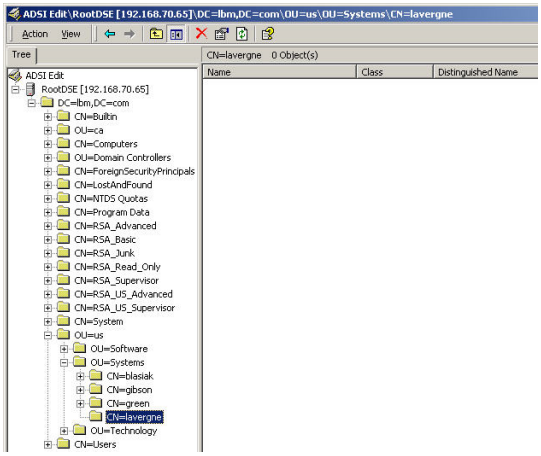


7. Wählen Sie die Registerkarte **Attributes** und klicken Sie dann auf **Add** (Hinzufügen). Das Fenster "Select Schema Object" (Schemaobjekt auswählen) wird geöffnet.

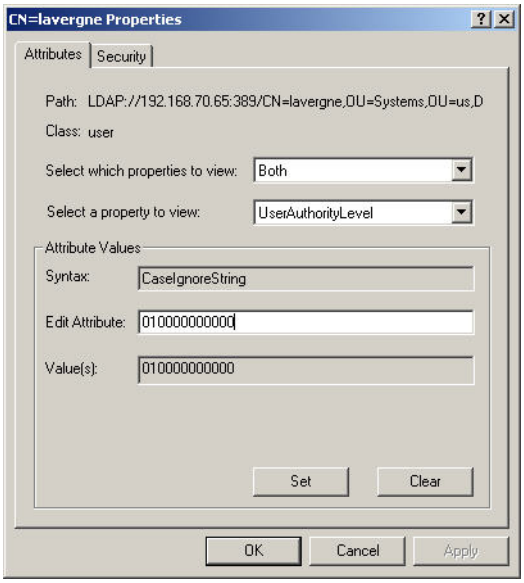


8. Blättern Sie abwärts auf **UserAuthorityLevel** und klicken Sie auf **OK**. Dieses Attribut wird nun in der Liste optionaler Attribute für die Benutzerobjektklasse auftauchen.
9. Wiederholen Sie die Schritte 6 auf Seite 66 bis 8 für die Klasse groups (Gruppen). Dies ermöglicht es, das Attribut **UserAuthorityLevel** einem Benutzer oder einer Benutzergruppe zuzuweisen. Dies sind die beiden einzigen Objektklassen, die dieses neue Attribut verwenden müssen.
10. Weisen Sie das Attribut **UserAuthorityLevel** den entsprechenden Benutzern und Benutzergruppen zu. Verwenden Sie zum Angleichen des Schemas, das auf dem Novell eDirectory-Server definiert ist, die gleichen Werte wie im Abschnitt „Berechtigungsstufen einrichten” auf Seite 56. Sie können dazu das Tool "ADSI Edit" verwenden. Das Unterstützungstool ADSI Edit von Microsoft ist ein Snap-in-Tool von Microsoft Management Console (MMC), mit dessen Hilfe alle Objekte im Verzeichnis (darunter Schema- und Konfigurationsinformationen) angezeigt, Objekte geändert und Zugriffssteuerungslisten auf Objekte festgelegt werden können.

11. Nehmen Sie für dieses Beispiel an, dass Sie das Attribut **UserAuthorityLevel** zu Benutzer lavergne hinzufügen möchten. Verwenden Sie dazu ADSI Edit. Sie müssen die entsprechenden Berechtigungsnachweise erbringen, um eine Verbindung mit Active Directory herzustellen; andernfalls haben Sie möglicherweise nicht die richtigen Benutzerberechtigungen, um Objekte auf dem Server zu ändern. Die folgende Abbildung zeigt das Schema, wie es bei hergestellter Verbindung mit dem Server auf ADSI angezeigt wird.



12. Klicken Sie mit der rechten Maustaste auf **lavergne** und klicken Sie auf **Properties (Eigenschaften)**. Ein Fenster ähnlich dem in der folgenden Abbildung wird geöffnet.



13. Wählen Sie im Feld **Select which properties to view** (Eigenschaften zur Ansicht auswählen) **UserAuthorityLevel** aus.
14. Geben Sie im Feld **Edit Attribute** (Attribut bearbeiten) `IBMRBSPermissions=010000000000` ein, was so viel bedeutet wie "Administratorzugriff". Klicken Sie auf **Set** (Festlegen).
15. Klicken Sie auf **OK**.
16. Sie können dieses Attribut Benutzergruppen hinzufügen, indem Sie die gleichen Schritte für das Benutzergruppenobjekt durchführen, das Sie ändern möchten.

Konfiguration von Active Directory überprüfen

Bevor Sie versuchen, eine Verbindung zwischen dem LDAP-Client und Active Directory herzustellen (um Benutzer zu authentifizieren), rufen Sie das Active Directory-Schema in einem LDAP-Browser auf. Sie sollten mindestens die Abfragen ausgeben, die in der folgenden Tabelle aufgelistet sind, um die Berechtigungsstufen und Gruppenzugehörigkeiten zu überprüfen.

Tabelle 9. Berechtigungsstufen und Gruppenzugehörigkeiten überprüfen

Suche nach definiertem Namen	Filter	Attribute
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

LDAP-Client konfigurieren

Sie können das LDAP für die Authentifizierung der Managementmodulbenutzer konfigurieren. Das IMM unterstützt sowohl die lokale als auch die ferne Benutzerauthentifizierung. Für die lokale Authentifizierung werden die Daten auf der Seite "Login Profiles" (Anmeldeprofile) verwendet, um Benutzer zu authentifizieren. Mithilfe eines LDAP-Servers kann ein Managementmodul einen Benutzer durch Abfragen oder Durchsuchen eines LDAP-Verzeichnisses auf einem fernen LDAP-Server ohne Abfragen der lokalen Benutzerdatenbank authentifizieren.

Wenn Sie eine Form der fernen Authentifizierung verwenden, können Sie auswählen, ob die Berechtigungen für die einzelnen erfolgreich authentifizierten Benutzer entweder lokal oder auf der Grundlage von Daten erteilt werden, die auf dem für die ferne Authentifizierung verwendeten LDAP-Server gespeichert sind. Die Berechtigungen, die für einen Benutzer erteilt werden, geben die Aktionen an, die der jeweilige Benutzer ausführen kann, während er am IMM angemeldet ist. Die Authentifizierungsmethoden für ferne Systeme werden in den folgenden Themen beschrieben:

- Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen
- Rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory
- Traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP

Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen

Mithilfe der Active Directory-Authentifizierung können Sie die ferne LDAP-Authentifizierung mit lokaler Erteilung von Benutzerberechtigungen für Benutzer konfigurieren.

Anmerkung: Die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen kann nur bei einem Server in einer Active Directory-Umgebung angewendet werden.

Wenn die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen verwendet wird, werden die Active Directory-Server nur zum Authentifizieren von Benutzern, also zum Überprüfen der Berechtigungsnachweise für Benutzer, verwendet. Auf dem Active Directory-Server werden keine Berechtigungsdaten für einen bestimmten Benutzer gespeichert. Die im IMM gespeicherten Gruppenprofile müssen mit Berechtigungsdaten konfiguriert werden. Die zum Konfigurieren der Gruppenprofile verwendeten Berechtigungsdaten kön-

nen durch Abrufen von Daten zur Mitgliedschaft für einen Benutzer vom Active Directory-Server angefordert werden. Diese Daten zur Mitgliedschaft enthalten eine Liste der Gruppen, denen ein Benutzer angehört (verschachtelte Gruppen werden unterstützt). Die auf dem Active Directory-Server angegebenen Gruppen werden mit den auf dem IMM lokal konfigurierten Gruppennamen verglichen. Für jede Gruppe, zu der der Benutzer als Mitglied gehört, werden dem Benutzer Berechtigungen für die jeweilige Gruppe zugewiesen. Für jeden Gruppennamen, der auf dem IMM lokal konfiguriert ist, gibt es ein entsprechendes Berechtigungsprofil, das auch für die jeweilige Gruppe konfiguriert ist.

Das IMM unterstützt bis zu 16 lokal konfigurierte Gruppennamen. Jeder Gruppenname darf aus maximal 63 Zeichen bestehen. Eines der folgenden Attribute muss als Gruppenname konfiguriert werden, um mit den von den Active Directory-Servern abgerufenen Daten zur Gruppenmitgliedschaft abgeglichen werden zu können:

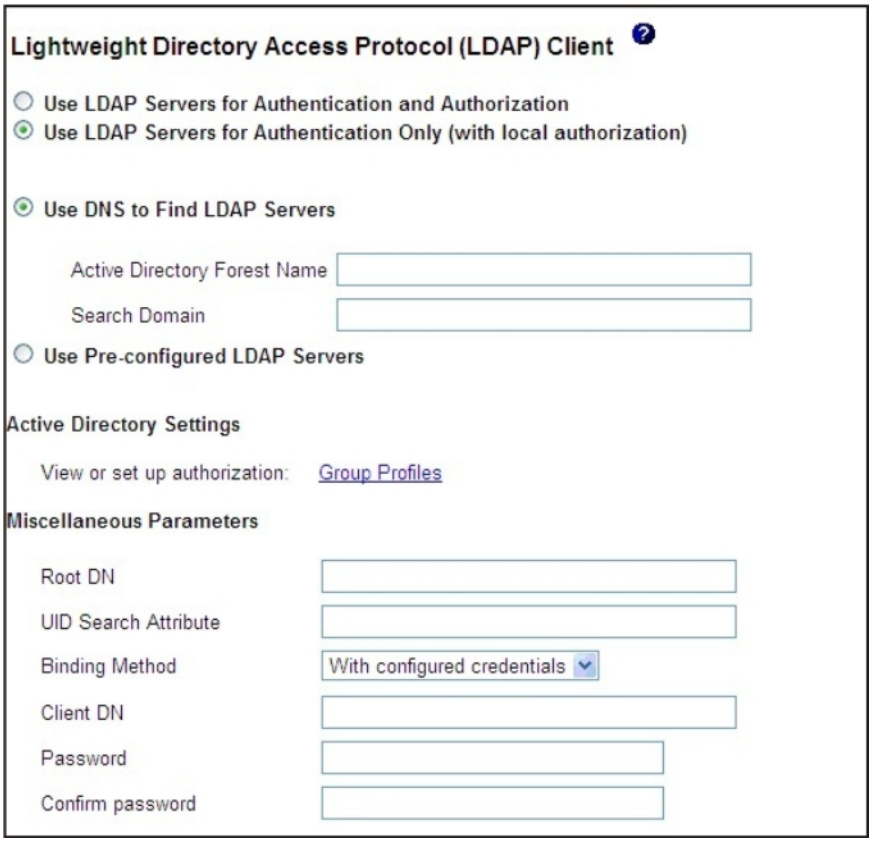
- Definierter Name (DN)
- Das Attribut "cn"
- Das Attribut "name"
- Das Attribut "sAMAccountName"

Gehen Sie wie folgt vor, um die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen für das IMM zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).
3. Wählen Sie **Use LDAP Servers for Authentication Only (with local authorization)** (Nur LDAP-Server für Authentifizierung verwenden (mit lokaler Erteilung von Berechtigungen)) aus.
4. Wählen Sie eine der folgenden Optionen aus, um die Domänencontroller manuell zu konfigurieren oder dynamisch zu ermitteln:
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die Domänencontroller anhand von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardauswahl) aus, um die Domänencontroller manuell zu konfigurieren.
5. Wenn Sie DNS zum dynamischen Ermitteln von Domänencontrollern verwenden, konfigurieren Sie zunächst die folgenden Einstellungen. Fahren Sie anschließend mit Schritt 7 auf Seite 71 fort.

   Anmerkung: Wenn Sie DNS zum dynamischen Ermitteln des Domänencontrollers verwenden, müssen Sie den vollständig qualifizierten Domänennamen des Domänencontrollers angeben.
   - Search Domain (Suchdomäne)
     - Geben Sie den Domänennamen des Domänencontrollers in das Feld **Search Domain** ein.
   - Active Directory Forest Name (Name der Active Directory-Gesamtstruktur)
     - Dieses optionale Feld wird zum Ermitteln globaler Kataloge verwendet. Globale Kataloge werden für Benutzer benötigt, die universellen Gruppen in mehreren Domänen angehören. In Umgebungen, in denen eine domänenübergreifende Gruppenzugehörigkeit nicht zulässig ist, muss dieses Feld nicht ausgefüllt werden.

In der folgenden Abbildung ist das Fenster "LDAP Client" dargestellt, wenn DNS zum dynamischen Ermitteln von Domänencontrollern verwendet wird.



6. Wenn Sie die Domänencontroller und globalen Kataloge manuell konfigurieren, verwenden Sie die Option **Use Pre-Configured LDAP Servers** (Standardauswahl). Konfigurieren Sie dann die Felder **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers) und **Port**.

   Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier Domänencontroller konfiguriert werden. Server für globalen Kataloge verwenden die Portnummer 3268 oder 3269. Die Verwendung einer anderen Portnummer gibt an, dass ein Domänencontroller konfiguriert wurde.

7. Wenn Sie Gruppenberechtigungsprofile verwenden, klicken Sie auf **Group Profiles** (Gruppenprofile) im Abschnitt "Active Directory Settings" (Active Directory-Einstellungen), um sie anzuzeigen oder zu konfigurieren (weitere Informationen hierzu finden Sie im Abschnitt „Gruppenprofile für Active Directory-Benutzer” auf Seite 74).

8. Kehren Sie zur Seite "Network Protocols" zurück. Klicken Sie auf den Link **LDAP Client section of the Network Protocols page** auf der Seite "Group Profiles for Active Directory Users" und blättern Sie zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client**.

9. Konfigurieren Sie alle sonstigen Parameter für das IMM. Die folgende Tabelle enthält Informationen zu diesen Parametern.

Tabelle 10. Sonstige Parameter

Feld	Beschreibung	Option
Root DN (Definierter Name des Stammele-ments)	Das IMM verwendet das Feld **Root DN** im DN-Format als Stammeintrag der Verzeichnisbaumstruktur. Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet. Beispiel: `dc=mycompany,dc=com`.	

Tabelle 10. Sonstige Parameter (Forts.)

Feld	Beschreibung	Option
Binding method (Bindungs-methode)	Das Feld **Binding Method** wird für einleitende Verbindungen zum Domänencontroller-Server verwendet. Wählen Sie eine der Optionen aus.	• With configured credentials (Mit konfiguriertem Berechtigungsnachweis): Geben Sie den definierten Namen und das Kennwort des Clients ein, die für die einleitende Verbindung verwendet werden sollen. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach einem Benutzersatz gesucht, der mit dem im Feld **Client DN** (Definierter Name des Clients) eingegebenen Namen übereinstimmt. Bei der Suche wird in der Regel nach allgemeinen Attributen gesucht, die mit der bei der Anmeldung eingegebenen Benutzer-ID übereinstimmen. Zu diesen Attributen zählen die Attribute "displayName", "sAMAccountName" und "userPrincipalName". Wenn das Feld **UID search attribute** (Suchattribut für Benutzer-ID) konfiguriert wird, bezieht sich die Suche darüber hinaus auch auf dieses Attribut. Wenn die Suche erfolgreich ist, wird versucht, eine zweite Verbindung, diesmal mit dem definierten Benutzernamen (über die Suche abgerufen) und dem bei der Anmeldung angegebenen Kennwort, herzustellen. Wenn die zweite Verbindung hergestellt werden kann, verläuft die Authentifizierung erfolgreich und die Daten zur Gruppenzugehörigkeit für den Benutzer werden abgerufen und mit den auf dem IMM konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden. • With login credentials (Mit Berechtigungsnachweise für Anmeldung): Die einleitende Verbindung mit dem Server des Domänencontrollers wird mithilfe des bei der Anmeldung angegebenen Berechtigungsnachweises hergestellt. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach dem Benutzersatz gesucht. Sobald dieser gefunden ist, werden die Daten zur Gruppenzugehörigkeit für den Benutzer abgerufen und mit den auf dem IMM konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden. • Anonymously (Anonym): Die einleitende Verbindung mit dem Server des Domänencontrollers wird ohne einen definierten Namen und Kennwort hergestellt. Diese Option sollte nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen.

Gruppenprofile für Active Directory-Benutzer

Gruppenprofile werden konfiguriert, um Spezifikationen für eine lokale Erteilung von Berechtigungen für Benutzergruppen bereitzustellen. Jedes Gruppenprofil umfasst eine Erteilung von Berechtigungen, die als Berechtigungsstufe (Rolle) ausgedrückt wird, genau wie in einem Anmeldeprofil. Zum Konfigurieren von Gruppenprofilen müssen die betreffenden Benutzer über die Berechtigung zur Benutzerkontenverwaltung verfügen. Um Benutzern Gruppenprofile zuordnen zu können, sind Server für eine LDAP-Authentifizierung erforderlich.

Liste der Gruppenprofile

Auf die Liste der Gruppenprofile können Sie zugreifen, indem Sie auf **IMM Control** > **Login Profiles** (IMM-Steuerung - Anmeldeprofile) klicken. Für jedes Gruppenprofil werden die Gruppen-ID und eine Rollenzusammenfassung angezeigt (wie für Anmeldeprofile). Von dieser Liste ausgehend können Sie neue Gruppen hinzufügen und bereits vorhandene Gruppen auswählen, um sie zu bearbeiten oder zu löschen.

In der folgenden Abbildung ist das Fenster "Group Profiles for Active Directory Users" (Gruppenprofile für Active Directory-Benutzer) dargestellt.

Um ein Gruppenprofil zu bearbeiten, klicken Sie auf **Edit**. Für die betreffende Gruppe wird die Seite "Group Profile" geöffnet. Um ein Gruppenprofil zu löschen, klicken Sie auf **Delete**. Sie müssen das Löschen eines Gruppenprofils bestätigen. Um ein neues Gruppenprofil hinzuzufügen, klicken Sie auf den Link **Add a group** (Gruppe hinzufügen). Die Seite "Group Profile" wird geöffnet, sodass Sie die Informationen für das neue Gruppenprofil eingeben können. Sie können maximal 16 Gruppenprofile hinzufügen. Die Gruppenprofilnamen müssen nicht eindeutig sein.

In der folgenden Tabelle werden die Felder auf der Seite "Group Profile" beschrieben.

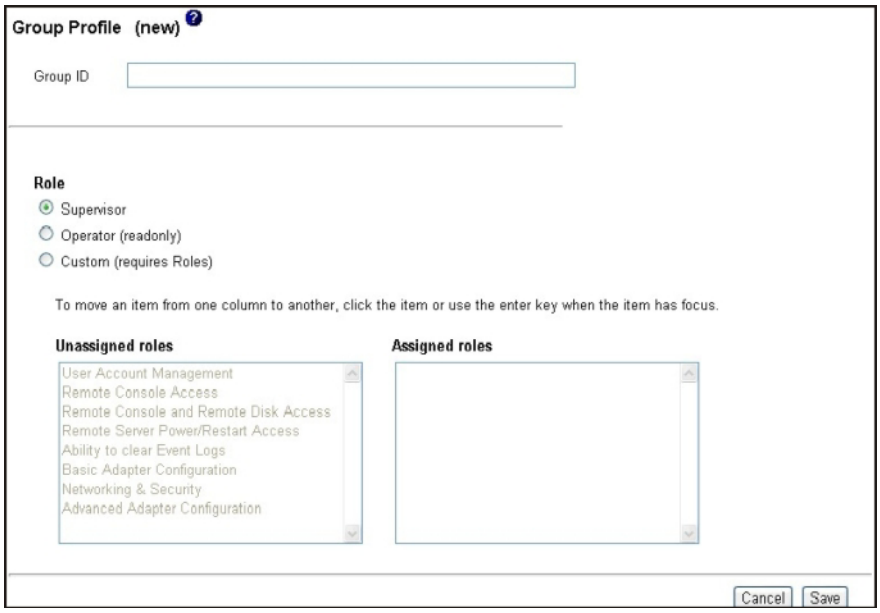
Tabelle 11. Informationen zu Gruppenprofilen

Feld	Option	Beschreibung
Group ID (Gruppen-ID)		In diesem Feld wird die Gruppen-ID für das Gruppenprofil angegeben. Sie können höchstens 63 Zeichen eingeben. Die Gruppen-ID muss dieselbe sein wie ihre Entsprechungen auf den LDAP-Servern. Beispiele für Gruppennamen: "IMM Admin Group" und "IMM/Robert".
Role (Rolle)		Wählen Sie die Rollen (Berechtigungsstufen) aus, die dieser Anmelde-ID zugeordnet sind, und übertragen Sie sie in das Feld **Assigned roles** (Zugeordnete Rollen). Mit der Eingabetaste oder einem Mausklick können Sie die ausgewählten Elemente von einem Feld in das andere übertragen.
	Supervisor (Administrator)	Für den Benutzer gelten keine Einschränkungen, es sei denn, ihm ist nur ein bestimmter Bereich zugeordnet.
	Operator (Bediener)	Der Benutzer verfügt nur über eine Lesezugriffsberechtigung und kann keine Änderungen durchführen, wie z. B. Speichern, Ändern oder Löschen. Dies gilt auch für Operationen, die den Status des IMM betreffen, wie z. B. den Neustart des IMM, das Wiederherstellen von Standardwerten und das Durchführen von Upgrades für die Firmware.
Role (Rolle)	Custom (Angepasst)	Der Benutzer unterliegt möglicherweise Einschränkungen, je nachdem, welche angepasste Berechtigungsstufe dem Benutzer zugeordnet wurde. Wenn Sie die Option "Custom" auswählen, müssen Sie mindestens eine der folgenden angepassten Berechtigungsstufen auswählen: • Networking and Security (Netzbetrieb und Sicherheit) – Der Benutzer kann die Konfiguration in den Anzeigen "Security", "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Portzuordnungen) und "Serial Port" (Serieller Anschluss) ändern. • User account management (Benutzerkontenverwaltung) – Der Benutzer kann andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) in der Anzeige "Login Profiles" (Anmeldeprofile) ändern. • Remote Console Access (Zugriff auf ferne Konsole) – Der Benutzer kann auf die Remote-Server-Konsole zugreifen. • Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger) – Der Benutzer kann auf die Remote-Server-Konsole und die fernen Datenträgerfunktionen für den fernen Server zugreifen.

Tabelle 11. Informationen zu Gruppenprofilen (Forts.)

Feld	Option	Beschreibung
		• Remote Server Power/Restart Access (Zugriff auf Einschalten/Neustart des fernen Servers) – Der Benutzer kann auf die Einschalt-, Neustart- und Serverzeitlimitfunktionen für den fernen Server zugreifen. • Basic Adapter Configuration (Basisadapterkonfiguration) – Der Benutzer kann Konfigurationsparameter in den Anzeigen "System Settings" (Systemeinstellungen) (ausgenommen "Contact", "Location" und "Server Timeouts") und "Alerts" ändern. • Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen) – Der Benutzer kann die Ereignisprotokolle löschen. **Anmerkung:** Alle Benutzer können die Ereignisprotokolle anzeigen. Zum Löschen der Ereignisprotokolle ist jedoch diese Berechtigung erforderlich. • Advanced Adapter Configuration (Erweiterte Adapterkonfiguration) – Der Benutzer ist beim Konfigurieren des Adapters nicht eingeschränkt und hat Verwaltungszugriff auf das IMM. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE-Netzboot, werkseitige Adaptervoreinstellungen wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wiederherstellen und den Adapter erneut starten bzw. zurücksetzen. **Anmerkung:** Diese Berechtigungsstufe schließt jedoch die Funktion "Server Power/Restart Control" (Steuerung von Einschalten/Neustart des Servers) und die Zeitlimitfunktion aus.
Anmerkung: Um eine Situation zu verhindern, in der kein Benutzer Schreib-/Lesezugriff hat, muss für Anmeldeprofil 1 mindestens die Fähigkeit zum Ändern der Anmeldeprofile definiert werden. Diesem Benutzer muss die Zugriffsberechtigung "Supervisor" oder die Zugriffsberechtigung "User Account Management" erteilt werden. Dadurch wird sichergestellt, dass zumindest ein Benutzer Aktionen ausführen, Konfigurationsänderungen vornehmen und Benutzer zu den Anmeldeprofilen hinzufügen kann, die dann wiederum Aktionen ausführen oder Konfigurationsänderungen vornehmen können.		

In der folgenden Abbildung ist das Fenster "Group Profile" (Gruppenprofil) dargestellt.



Rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory

Mithilfe von Active Directory können Sie die ferne Authentifizierung und Erteilung von Berechtigungen mittels LDAP für Benutzer konfigurieren.

Anmerkungen:

- Die rollenbasierte Active Directory-Authentifizierung und Erteilung von Berechtigungen kann nur bei einem Server in einer Active Directory-Umgebung angewendet werden.
- Für die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory ist das Snap-in für die erweiterte rollenabhängige Sicherheit erforderlich.

Für die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory werden auf einem Active Directory-Server gespeicherte Konfigurationsdaten verwendet, um einen Benutzer zu authentifizieren und dem Benutzer anschließend Berechtigungen zuzuweisen. Verwenden Sie vor dem Aktivieren der rollenabhängigen Authentifizierung und Erteilung von Berechtigungen mittels Active Directory das Snap-in für die erweiterte rollenabhängige Sicherheit, um die Konfigurationsdaten auf dem Active Directory-Server zu speichern, der Benutzern Berechtigungen zuweist. Dieses Snap-in kann auf jedem Microsoft Windows-Client ausgeführt und von der Website "http://www.ibm.com/systems/support/" heruntergeladen werden.

Mithilfe des Snap-ins für die erweiterte rollenabhängige Sicherheit können Sie auf einem Active Directory-Server Rollen konfigurieren und diese Rollen dem IMM, Benutzern und Gruppen zuweisen. Informationen und Anweisungen hierzu finden Sie in der Dokumentation zum Snap-in für die erweiterte rollenabhängige Sicherheit. Rollen geben die Benutzern und Gruppen zugewiesenen Berechtigungen sowie die Befehlsziele, wie z. B. das IMM oder einen Blade-Server, an, denen eine Rolle zugeordnet ist. Bevor die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory aktiviert werden kann, müssen auf dem Active Directory-Server Rollen konfiguriert werden.

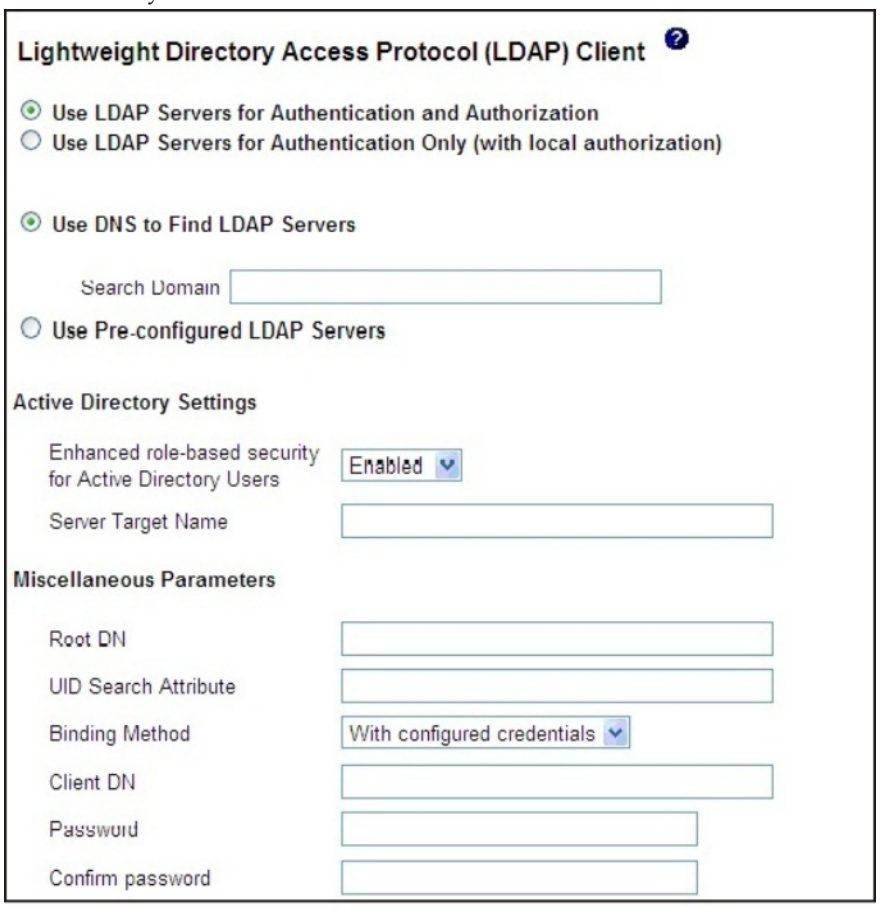
Der im Feld **Server Target Name** (Serverzielname) konfigurierte optionale Name gibt ein bestimmtes IMM an und kann mithilfe des Snap-ins für die rollenabhängige Sicherheit auf dem Active Directory-Server einer oder mehreren Rollen zugewiesen werden. Hierzu müssen verwaltete Ziele erstellt, diesen bestimmte Namen und anschließend die entsprechenden Rollen zugewiesen werden. Ein konfigurierter Serverzielname kann bestimmte Rollen für Benutzer und IMM-Ziele definieren, die derselben Rolle angehören. Wenn sich ein Benutzer beim IMM anmeldet und er mittels Active Directory authentifiziert wird, werden die Rollen für diesen Benutzer aus dem Verzeichnis abgerufen. Die Berechtigungen, die dem Benutzer zugewiesen werden, werden aus den Rollen extrahiert, die über ein Ziel als Mitglied mit einem Namen verfügen, der dem des IMM entspricht, oder die über ein Ziel verfügen, das einem beliebigen IMM entspricht. Einem IMM kann ein eindeutiger Name zugewiesen werden. Es ist aber auch möglich, dass mehrere IMMs denselben Zielnamen verwenden. Wenn mehreren IMMs derselbe Zielname zugewiesen wird, werden die IMMs dadurch zusammengefasst und sie werden derselben Rolle zugeordnet.

Gehen Sie wie folgt vor, um die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory für das IMM zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).
3. Wählen Sie **Use LDAP Servers for Authentication and Authorization** (LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden) aus.

4. Wählen Sie **Enabled** (Aktiviert) für das Feld **Enhanced role-based security for Active Directory Users** (Erweiterte, rollenbasierte Sicherheit für Active Directory-Benutzer) aus.
5. Wählen Sie eine der folgenden Optionen aus, um die Domänencontroller dynamisch zu ermitteln oder manuell zu konfigurieren:
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die Domänencontroller anhand von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardauswahl) aus, um die Domänencontroller manuell zu konfigurieren.
6. Wenn Sie DNS zum dynamischen Ermitteln von Domänencontrollern verwenden, konfigurieren Sie zunächst den Domänennamen des Domänencontrollers. Fahren Sie anschließend mit Schritt 8 auf Seite 80 fort. Sie müssen den vollständig qualifizierten Domänennamen des Domänencontrollers angeben. Geben Sie den Domänennamen des Domänencontrollers in das Feld **Search Domain** ein.

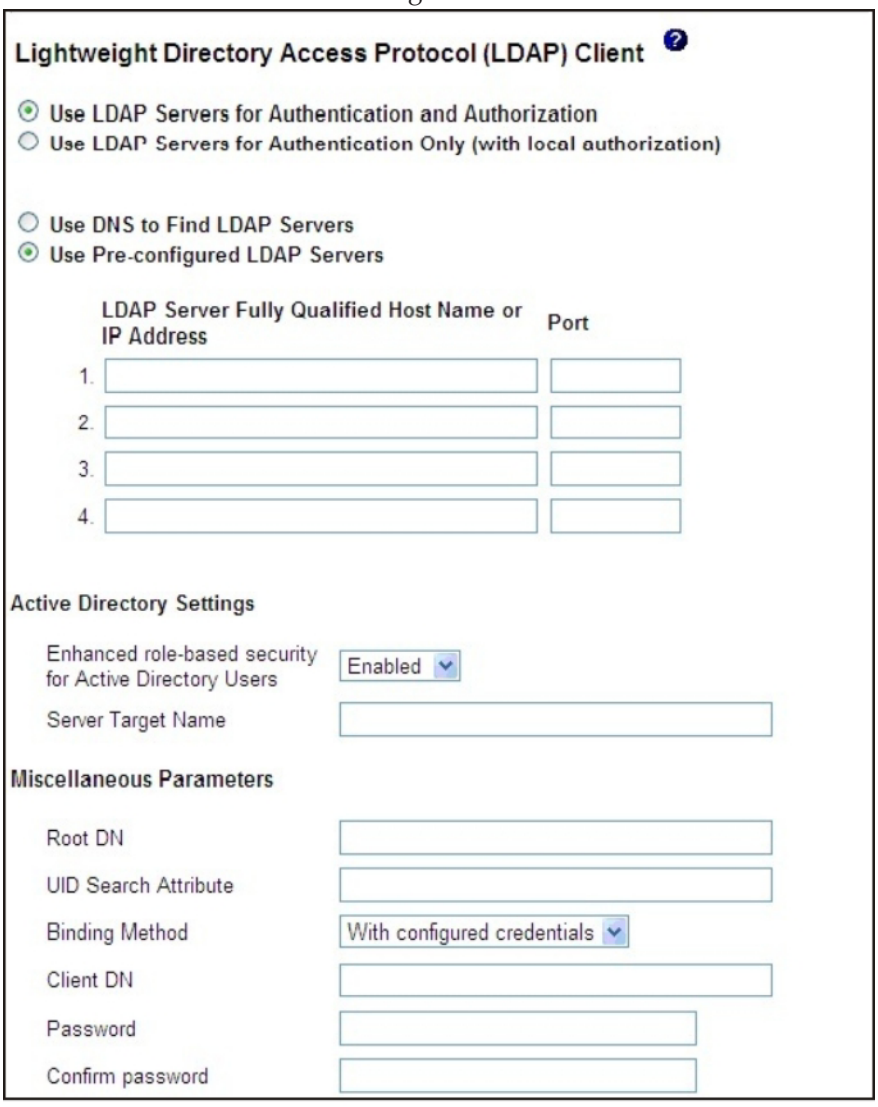
   In der folgenden Abbildung ist das Fenster "LDAP Client" dargestellt, wenn DNS zum dynamischen Ermitteln von Domänencontrollern verwendet wird.



7. Wenn Sie die Domänencontroller manuell konfigurieren, konfigurieren Sie zunächst die Felder **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers) und **Port** (Port).

   Anmerkung: Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier Domänencontroller konfiguriert werden.

In der folgenden Abbildung ist das Fenster "LDAP Client" dargestellt, wenn die Domänencontroller manuell konfiguriert werden.



8. Konfigurieren Sie die Active Directory-Einstellungen, indem Sie **Enabled** im Menü **Enhanced role-based security for Active Directory Users** auswählen.
9. Konfigurieren Sie alle sonstigen Parameter. Die folgende Tabelle enthält Informationen zu diesen Parametern.

Tabelle 12. Sonstige Parameter

Feld	Beschreibung	Option
Root DN (Definierter Name des Stammelements)	Das IMM verwendet das Feld **Root DN** (Definierter Name des Stammelements) im DN-Format als Stammeintrag der Verzeichnisbaumstruktur. Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet. Beispiel: `dc=mycompany,dc=com`.	

Tabelle 12. Sonstige Parameter (Forts.)

Feld	Beschreibung	Option
Binding method (Bindungs-methode)	Das Feld **Binding Method** wird für einleitende Verbindungen zum Domänencontroller-Server verwendet. Wählen Sie eine der Optionen aus.	• Anonymously (Anonym): Die einleitende Verbindung mit dem Server des Domänencontrollers wird ohne einen definierten Namen und Kennwort hergestellt. Diese Option sollte nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen. • With configured credentials (Mit konfiguriertem Berechtigungsnachweis): Geben Sie den definierten Namen und das Kennwort des Clients ein, die für die einleitende Verbindung verwendet werden sollen. • With login credentials (Mit Berechtigungsnachweise für Anmeldung): Die einleitende Verbindung mit dem Server des Domänencontrollers wird mithilfe des bei der Anmeldung angegebenen Berechtigungsnachweises hergestellt. Die Benutzer-ID kann als definierter Name, als Teil eines definierten Namens, als vollständig qualifizierter Domänenname oder über eine Benutzer-ID angegeben werden, die mit den Daten im Feld **UID Search Attribute** übereinstimmt, das auf dem IMM konfiguriert wurde. Wenn der Berechtigungsnachweis einem Teil eines definierten Namen ähnelt (wie z. B. `cn=joe`), wird dieser Teil eines definierten Namens als Präfix zum konfigurierten definierten Namen des Stammelements hinzugefügt, in dem Versuch, einen definierten Namen zu erstellen, der mit dem Datensatz des Benutzers übereinstimmt. Wenn der Bindungsversuch fehlschlägt, wird im letzten Bindungsversuch das Präfix `cn=` zum Berechtigungsnachweis für Anmeldung hinzugefügt. Anschließend werden die Ergebnisse der Zeichenfolge zum definierten Namen des konfigurierten Stammelements hinzugefügt.

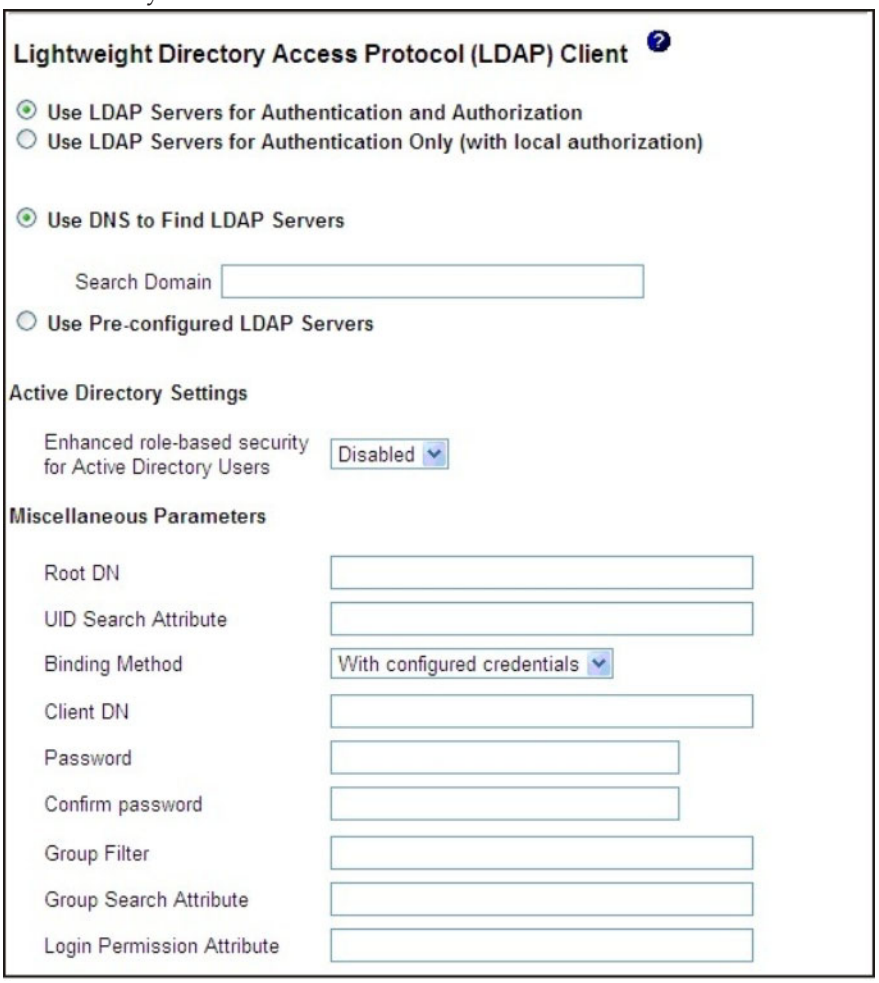
Traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP

Die traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP ist das ursprünglich mit dem IMM verwendete Modell. Die traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP unterstützt Active Directory-, Novell eDirectory- und OpenLDAP-Umgebungen und verwendet auf einem LDAP-Server gespeicherte Konfigurationsdaten, um Benutzern Berechtigungen zuzuweisen. Die traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP wird verwendet, um Benutzer über einen LDAP-Server zu authentifizieren und um Benutzern über einen LDAP-Server Berechtigungen zu erteilen. Wenn die erweiterte, rollenbasierte Sicherheit für Active Directory-Benutzer auf dem IMM inaktiviert ist, können Sie die LDAP-Suchattribute für das IMM konfigurieren.

Gehen Sie wie folgt vor, um eine traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP für das IMM zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).
3. Wählen Sie **Use LDAP Servers for Authentication and Authorization** (LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden) aus.
4. Wählen Sie **Disabled** (Inaktiviert) für das Feld **Enhanced role-based security for Active Directory Users** (Erweiterte, rollenbasierte Sicherheit für Active Directory-Benutzer) aus.
5. Wählen Sie eine der folgenden Optionen aus, um die LDAP-Server für die Authentifizierung dynamisch zu ermitteln oder manuell zu konfigurieren:
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die LDAP-Server anhand von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardauswahl) aus, um die LDAP-Server manuell zu konfigurieren.
6. Wenn Sie DNS zum dynamischen Ermitteln von LDAP-Servern verwenden, konfigurieren Sie zunächst den Domänennamen des LDAP-Servers. Fahren Sie anschließend mit Schritt 8 auf Seite 84 fort. Sie müssen den vollständig qualifizierten Domänennamen des LDAP-Servers angeben. Geben Sie den Domänennamen des LDAP-Servers in das Feld **Search Domain** ein.

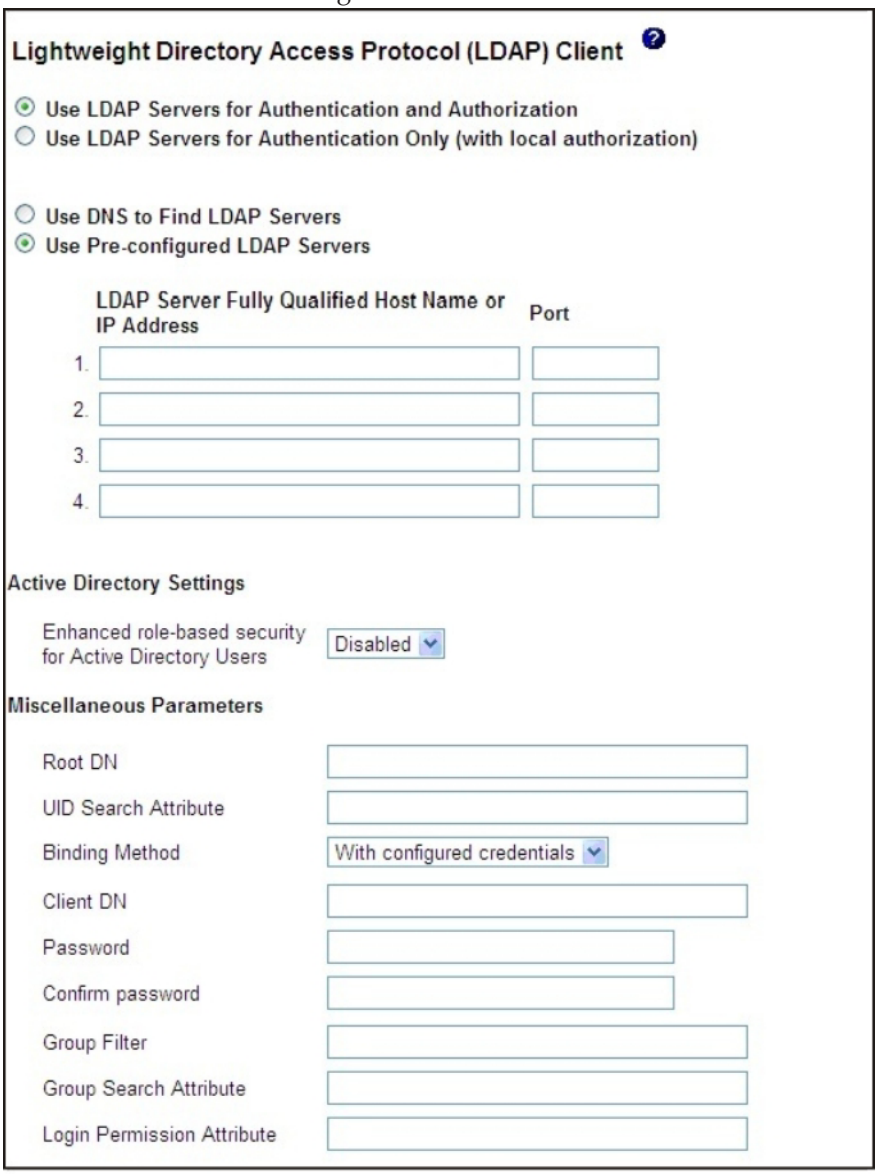
In der folgenden Abbildung ist das Fenster "LDAP Client" dargestellt, wenn DNS zum dynamischen Ermitteln von LDAP-Servern verwendet wird.



7. Wenn Sie die LDAP-Server manuell konfigurieren, konfigurieren Sie zunächst die Felder **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers) und **Port**. Fahren Sie anschließend mit Schritt 8 auf Seite 84 fort.

   Anmerkung: Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier LDAP-Server konfiguriert werden.

In der folgenden Abbildung ist das Fenster "LDAP Client" dargestellt, wenn die LDAP-Server manuell konfiguriert werden.



8. Konfigurieren Sie die Active Directory-Einstellungen, indem Sie **Disabled** im Menü **Enhanced role-based security for Active Directory Users** auswählen.
9. Konfigurieren Sie alle sonstigen Parameter. In der folgenden Liste finden Sie Beschreibungen der erforderlichen Parameterfelder.
   - Das IMM verwendet das Feld **Root DN** (Definierter Name des Stammelements) im DN-Format als Stammeintrag der Verzeichnisbaumstruktur. Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet. Beispiel: `dc=mycompany,dc=com`.
   - Das Feld **Binding Method** (Bindungsmethode) wird für einleitende Verbindungen zum Domänencontroller-Server verwendet. Verwenden Sie eine der folgenden Bindungsoptionen:
     – Anonymously (Anonym):

       Die einleitende Verbindung mit dem Server des Domänencontrollers wird ohne einen definierten Namen und Kennwort hergestellt. Diese Option sollte nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen.

– With configured credentials (Mit konfiguriertem Berechtigungsnachweis):
  Geben Sie den definierten Namen und das Kennwort des Clients ein, die für die einleitende Verbindung verwendet werden sollen.
– With login credentials (Mit Berechtigungsnachweise für Anmeldung):
  Bindung mit dem Berechtigungsnachweis, der beim Anmeldeprozess angegeben wird. Die Benutzer-ID kann als definierter Name, als Teil eines definierten Namens, als vollständig qualifizierter Domänenname oder über eine Benutzer-ID angegeben werden, die mit den Daten im Feld **UID Search Attribute** übereinstimmt, das auf dem IMM konfiguriert wurde. Wenn der Berechtigungsnachweis einem Teil eines definierten Namen ähnelt (wie z. B. `cn=joe`), wird dieser Teil eines definierten Namens als Präfix zum konfigurierten definierten Namen des Stammelements hinzugefügt, in dem Versuch, einen definierten Namen zu erstellen, der mit dem Datensatz des Benutzers übereinstimmt. Wenn der Bindungsversuch fehlschlägt, wird im letzten Bindungsversuch das Präfix `cn=` zum Berechtigungsnachweis für Anmeldung hinzugefügt. Anschließend werden die Ergebnisse der Zeichenfolge zum definierten Namen des konfigurierten Stammelements hinzugefügt.

- Das Feld **Group Filter** (Gruppenfilter) wird für die Gruppenauthentifizierung verwendet. Es gibt die Gruppe an, zu der das IMM gehört. Wenn der Gruppenfilter leer ist, ist die Gruppenauthentifizierung automatisch erfolgreich. Die Gruppenauthentifizierung (falls aktiviert) wird nach der Benutzerauthentifizierung durchgeführt. Dabei wird versucht, mindestens eine Gruppe im Gruppenfilter zu finden, die mit einer Gruppe übereinstimmt, der der Benutzer angehört. Wenn es keine Übereinstimmung gibt, schlägt die Authentifizierung des Benutzers fehl und der Zugriff wird verweigert. Wenn mindestens eine Übereinstimmung vorhanden ist, ist die Gruppenauthentifizierung erfolgreich. Beim Abgleich muss die Groß-/Kleinschreibung beachtet werden.

  Wenn die Gruppenauthentifizierung inaktiviert ist, müssen der eigene Datensatz des Benutzers das Berechtigungsattribut enthalten. Andernfalls wird der Zugriff verweigert. Dem Benutzer werden die Berechtigungen zugewiesen, die mit der Gruppe verknüpft sind, die dem Filter entspricht. Die mit einer Gruppe verknüpften Berechtigungen werden durch Abrufen der Daten unter **Login Permission Attribute** (Attribut für die Anmeldeberechtigung) gesucht.

  Der Filter ist auf 511 Zeichen begrenzt und enthält einen oder mehrere Gruppennamen. Der Doppelpunkt (:) wird verwendet, um mehrere Gruppennamen anzugeben. Vorangestellte und nachgestellte Leerzeichen werden nicht beachtet. Alle anderen Leerzeichen werden als Teil des Gruppennamens behandelt. Ein Gruppenname kann als vollständiger definierter Name oder nur mithilfe des *cn*-Teils angegeben werden. Beispiel: Eine Gruppe mit dem definierten Namen `cn=adminGroup,dc=mycompany,dc=com` kann mit dem tatsächlichen definierten Namen oder mit "adminGroup" angegeben werden.

  Anmerkung: Das zuvor verwendete Sternsymbol (*) wird nicht mehr als Platzhalterzeichen behandelt. Das Platzhalterzeichen wurde aus Sicherheitsgründen entfernt.
- Das Feld **Group Search Attribute** (Gruppensuchattribut) wird vom Suchalgorithmus für die Suche nach Gruppenzugehörigkeitsdaten für einen bestimmten Benutzer verwendet. Wenn der Gruppenfiltername konfiguriert wurde, muss die Liste der Gruppen, denen der Benutzer angehört, vom LDAP-Server abgerufen werden. Diese Liste ist zum Ausführen der Gruppenauthentifizierung erforderlich. Um diese Liste abzurufen, muss der an den LDAP-

Server gesendete Suchfilter den Attributnamen angeben, der den Gruppen zugeordnet wurde. Das Feld **Group Search Attribute** gibt den Attributnamen an.

In einer Active Directory- oder Novell eDirectory-Umgebung gibt das Feld **Group Search Attribute** den Attributnamen an, der die Gruppen bezeichnet, denen ein Benutzer angehört. In Active Directory wird das Attribut **memberOf** und in Novell eDirectory das Attribut **groupMembership** verwendet. In einer OpenLDAP-Serverumgebung werden Benutzer normalerweise Gruppen zugeordnet, deren objectClass gleich "PosixGroup" ist. In diesem Kontext gibt der Parameter "Group Search Attribut" den Attributnamen an, der die Mitglieder einer bestimmten "PosixGroup" bezeichnet, meist **memberUid**. Wenn im Feld **Group Search Attribute** keine Angaben gemacht werden, wird für den Attributnamen im Filter standardmäßig **memberOf** verwendet.

- Das Feld **Login Permission Attribute** (Anmeldeberechtigungsattribut) gibt den Attributnamen an, der den Anmeldeberechtigungen für den Benutzer zugeordnet ist. Wenn ein Benutzer erfolgreich mithilfe eines LDAP-Servers authentifiziert wird, müssen die Anmeldeberechtigungen für diesen Benutzer abgerufen werden.

  Anmerkung: Das Feld **Login Permission Attribute** muss ausgefüllt werden, andernfalls ist es nicht möglich, die Benutzerberechtigungen abzurufen. Ohne bestätigte Berechtigungen schlägt der Anmeldeversuch fehl.

  In dem vom LDAP-Server zurückgegebenen Attributwert wird nach der Suchbegriffszeichenfolge `IBMRBSPermissions=` gesucht. Diesem Suchbegriff folgt unmittelbar eine Bitfolge (aus bis zu 12 aufeinanderfolgenden Nullen oder Einsen). Jedes Bit steht für eine bestimmte Gruppe von Funktionen. Die Bits sind entsprechend ihrer Position nummeriert. Das erste Bit (links) ist Bitposition 0, das letzte Bit (rechts) ist Bitposition 11. Der Wert 1 in einer bestimmten Position aktiviert diese betreffende Funktion. Der Wert 0 inaktiviert diese Funktion. Die Zeichenfolge `IBMRBSPermissions=010000000000` ist ein Beispiel für ein Attribut.

  Das Schlüsselwort `IBMRBSPermissions=` kann in einer beliebigen Position im Feld **Login Permission Attribute** positioniert werden. So kann der LDAP-Administrator ein vorhandenes Attribut wiederverwenden, eine Erweiterung des LDAP-Schemas verhindern und ermöglichen, dass das Attribut für seine ursprüngliche Bestimmung verwendet wird. Der Benutzer kann nun die Schlüsselwortzeichenfolge an den Anfang, ans Ende oder in einer beliebigen anderen Position in dieses Feld hinzufügen. Das verwendete Attribut lässt eine frei formatierte Zeichenfolge zu.

  In der folgenden Tabelle wird jede Bitposition erklärt.

Tabelle 13. Berechtigungsbits

Bit-position	Funktion	Erläuterung
0	Deny Always (Nie zulassen)	Wenn dieses Bit gesetzt ist, wird die Authentifizierung eines Benutzers immer fehlschlagen. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.

Tabelle 13. Berechtigungsbits (Forts.)

Bit-position	Funktion	Erläuterung
1	Supervisor Access (Administratorzugriff)	Wenn dieses Bit gesetzt ist, wird einem Benutzer die Administratorberechtigung erteilt. Der Benutzer hat Schreib-/Lesezugriff auf jede Funktion. Wenn Sie dieses Bit einstellen, müssen Sie die anderen Bits nicht einzeln einstellen.
2	Read Only Access (Schreibgeschützter Zugriff)	Wenn dieses Bit gesetzt ist, hat ein Benutzer schreibgeschützten Zugriff und kann keine Wartungsarbeiten durchführen (beispielsweise Neustart, fern ausgeführte Aktionen oder Firmwareaktualisierungen). Nichts kann durch Speicher-, Lösch- oder Wiederherstellungsfunktionen geändert werden. Bitposition 2 und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung hat. Wenn irgendein anderes Bit eingestellt ist, wird dieses Bit ignoriert.
3	Networking (Netzbetrieb) & Security	Wenn dieses Bit gesetzt ist, kann ein Benutzer die Konfiguration in den Anzeigen "Security", "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Anschlusszuordnungen) und "Serial Port" (Serieller Anschluss) ändern.
4	User Account Management (Benutzerkontenverwaltung)	Wenn dieses Bit gesetzt ist, kann ein Benutzer andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) in der Anzeige "Login Profiles" (Anmeldeprofile) ändern.
5	Remote Console Access (Zugriff auf ferne Konsole)	Wenn dieses Bit gesetzt ist, hat ein Benutzer Zugriff auf die Remote-Server-Konsole und kann die Konfiguration in der Anzeige "Serial Port" ändern.
6	Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)	Wenn dieses Bit gesetzt ist, kann ein Benutzer auf die Remote-Server-Konsole und die fernen Datenträgerfunktionen für den fernen Server zugreifen. Der Benutzer kann außerdem die Konfiguration in der Anzeige "Serial Port" ändern.
7	Remote Server Power/Restart Access (Zugriff auf Einschalten/Neustart des fernen Servers)	Wenn dieses Bit gesetzt ist, kann ein Benutzer auf die Einschalt-, Neustart- und Serverzeitlimitfunktionen für den fernen Server zugreifen.

Tabelle 13. Berechtigungsbits (Forts.)

Bit-position	Funktion	Erläuterung
8	Basic Adapter Configuration (Basisadapterkonfiguration)	Wenn dieses Bit gesetzt ist, kann ein Benutzer Konfigurationsparameter in den Anzeigen "System Settings" (Systemeinstellungen) und "Alerts" ändern (ausgenommen die Parameter "Contact", "Location" und "Server Timeout" (Serverzeitlimit)).
9	Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)	Wenn dieses Bit gesetzt ist, kann ein Benutzer die Ereignisprotokolle löschen. **Anmerkung:** Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu können, muss der Benutzer diese Berechtigungsstufe haben.
10	Advanced Adapter Configuration (Erweiterte Adapterkonfiguration)	Wenn dieses Bit gesetzt ist, ist ein Benutzer beim Konfigurieren des Adapters nicht eingeschränkt und hat Verwaltungszugriff auf das IMM. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE-Netzboot, werkseitige Adaptervoreinstellungen wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wiederherstellen und den Adapter erneut starten bzw. zurücksetzen. Hiervon ausgenommen sind die Funktion "Server Power/Restart Control" (Steuerung von Einschalten/Neustart des Servers) und die Zeitlimitfunktion.
11	Reserved (Reserviert)	Diese Bitposition ist für den künftigen Gebrauch reserviert (zurzeit nicht relevant).

Anmerkungen:

- Wenn Bits nicht verwendet werden, wird der Standard für den Benutzer auf "Read Only" (Schreibgeschützt) eingestellt.
- Priorität haben die Anmeldeberechtigungen, die direkt aus dem Benutzersatz abgerufen werden. Wenn der Benutzersatz im Feld **Login Permission Attribute** (Anmeldeberechtigungsattribut) keinen Namen enthält, wird versucht, die Berechtigungen von den Gruppen abzurufen, denen der Benutzer angehört und die mit dem Gruppenfilter übereinstimmen. In diesem Fall wird dem Benutzer das inklusive ODER aller Bits für alle Gruppen zugewiesen.
- Wenn das Bit für "Deny Always" (Bitposition null) für irgendeine der Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit "Deny Always" hat vor allen anderen Bits Vorrang.
- Wenn ein Benutzer die Fähigkeit hat, allgemeine sowie Netzbetriebs- oder Sicherheits-Adapterkonfigurationsparameter zu ändern, sollten Sie erwägen, diesem Benutzer die Fähigkeit zu geben, das IMM erneut zu starten (Bitposition zehn). Ohne diese Fähigkeit kann ein Benutzer zwar möglicherweise einen Parameter ändern, dieser Parameter wird jedoch nicht wirksam.

Sicherheitsfunktionen konfigurieren

Sie können das in diesem Abschnitt beschriebene allgemeine Verfahren verwenden, um die Sicherheitsfunktionen für die Verschlüsselung sensibler Daten, für den IMM-Web-Server, für die Verbindung zwischen dem IMM und IBM Systems Director, für die Verbindung zwischen dem IMM und einem LDAP-Server und für die Verschlüsselungsverwaltung zu konfigurieren. Wenn Sie mit der Verwendung von SSL-Zertifikaten nicht vertraut sind, lesen Sie die Informationen im Abschnitt „SSL-Zertifikat" auf Seite 91.

Gehen Sie wie folgt vor, um die Sicherheitsfunktionen für das IMM zu konfigurieren:

1. Verschlüsselung für sensible Daten konfigurieren:
   a. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit). Blättern Sie zum Abschnitt **Enable Data Encryption** (Datenverschlüsselung aktivieren) und wählen Sie die Option **Enable** (Aktivieren) aus, um die Datenverschlüsselung zu aktivieren. Wählen Sie zum Inaktivieren der Datenverschlüsselung die Option **Disable** (Inaktivieren) aus.
2. Sicheren Web-Server konfigurieren:
   a. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit). Blättern Sie zum Bereich **HTTPS Server Configuration for Web Server** (HTTPS-Serverkonfiguration für Web-Server) und wählen Sie die Option **Disable** (Inaktivieren) aus, um den SSL-Server zu inaktivieren.
   b. Um ein Zertifikat zu generieren oder zu importieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **HTTPS Server Certificate Management** (Verwaltung von HTTPS-Serverzertifikaten). Weitere Informationen zum Verwalten von Zertifikaten finden Sie unter „Verwaltung von SSL-Serverzertifikaten" auf Seite 92.
   c. Um den SSL-Server zu aktivieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **HTTPS Server Configuration for Web Server** (HTTPS-Serverkonfiguration für Web-Server). Weitere Informationen zum Aktivieren von SSL finden Sie unter „SSL für den sicheren Web-Server oder IBM Systems Director über HTTPS aktivieren" auf Seite 97.
3. IBM Systems Director-Verbindung konfigurieren:
   a. Um die Einstellung **Systems Director over HTTPS** (IBM Systems Director über HTTPS) zu inaktivieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **IBM Systems Director over HTTPS Server Configuration** (Konfiguration von IBM Systems Director über HTTPS-Server).
   b. Um ein Zertifikat zu generieren oder zu importieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **IBM Systems Director over HTTPS Server Certificate Management** (IBM Systems Director über Verwaltung von HTTPS-Serverzertifikaten). Weitere Informationen finden Sie im Abschnitt „Verwaltung von SSL-Serverzertifikaten" auf Seite 92.
   c. Um den SSL-Server zu aktivieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **IBM Systems Director over HTTPS Server Configuration** (Konfiguration von IBM Systems Director über HTTPS-Server). Weitere Informationen zum Aktivieren von SSL finden Sie unter „SSL für den sicheren Web-Server oder IBM Systems Director über HTTPS aktivieren" auf Seite 97.
4. SSL-Sicherheit für LDAP-Verbindungen konfigurieren:

a. Um den SSL-Client zu inaktivieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client).
b. Um ein Zertifikat zu generieren oder zu importieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **SSL Client Certificate Management** (Verwaltung von SSL-Clientzertifikaten). Weitere Informationen finden Sie im Abschnitt „Verwaltung von SSL-Serverzertifikaten" auf Seite 92.
c. Um mindestens ein vertrauenswürdiges Zertifikat zu importieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **SSL Client Trusted Certificate Management** (SSL-Client-Verwaltung von vertrauenswürdigen Zertifikaten). Weitere Informationen finden Sie unter Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten.
d. Um den SSL-Client zu aktivieren, klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Abschnitt **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client). Weitere Informationen finden Sie im Abschnitt „SSL für den sicheren Web-Server oder IBM Systems Director über HTTPS aktivieren" auf Seite 97.

5. Verschlüsselungsverwaltung konfigurieren:
   a. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Bereich **Cryptography Management** (Verschlüsselungsverwaltung). Wählen Sie den **Basic Compatible Mode** (Basiskompatibilitätsmodus) aus.
   b. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit) und blättern Sie zum Bereich **Cryptography Management** (Verschlüsselungsverwaltung). Wählen Sie den **High Security Mode** (Hochsicherheitsmodus) aus.
6. Starten Sie das IMM erneut, damit die Änderungen an der SSL-Serverkonfiguration angewendet werden. Weitere Informationen hierzu finden Sie im Abschnitt „IMM erneut starten" auf Seite 103.

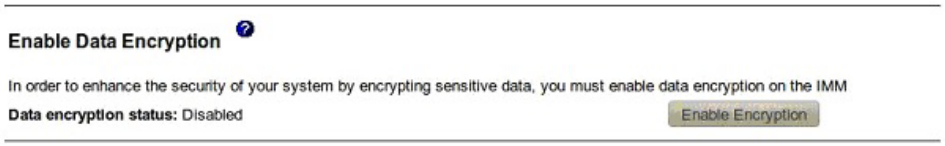
   Anmerkung: Änderungen an der Datenverschlüsselungskonfiguration und der SSL-Clientkonfiguration werden ohne Neustart des IMM sofort wirksam.

Datenverschlüsselung aktivieren

Standardmäßig werden sensible Daten unverschlüsselt gespeichert, damit sie mit der Vorgängerversion kompatibel bleiben. Um die Sicherheit Ihres Systems zu erhöhen, müssen Sie die Datenverschlüsselung auf dem IMM aktivieren.

Gehen Sie wie folgt vor, um die Datenverschlüsselung zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Security**.



2. Klicken Sie auf **Enable Encryption** (Verschlüsselung aktivieren), um die Datenverschlüsselung zu aktivieren.

   Anmerkung:

   - Wenn Sie die IMM-Firmwareversion 1.42 auf die Vorgängerversion herabstufen müssen, die keine Datenverschlüsselung bereitstellt, müssen Sie die Datenverschlüsselung inaktivieren, bevor Sie das Downgrade durchführen.

Wenn die Datenverschlüsselung vor dem Downgrade nicht inaktiviert wird, gehen die Kontoinformationen verloren.

- Wenn Sie die Datenverschlüsselung zu einem späteren Zeitpunkt inaktivieren müssen, wählen Sie die Option **Disable Encryption** (Verschlüsselung inaktivieren) aus, um die Datenverschlüsselung zu inaktivieren.

Web-Server, IBM Systems Director und sichere LDAP-Verbindung sichern

SSL (Secure Sockets Layer) ist ein Sicherheitsprotokoll, das eine geschützte Datenübertragung bereitstellt. SSL ermöglicht Client-/Serveranwendungen eine Datenübertragung, die gegen das Ausspionieren, das Manipulieren von Daten während der Übertragung und das Fälschen von Nachrichten geschützt ist.

Sie können das IMM so konfigurieren, dass die SSL-Unterstützung für zwei Verbindungsmöglichkeiten verwendet wird: den sicheren Server (HTTPS) und die sichere LDAP-Verbindung (LDAPS). Das IMM übernimmt je nach Verbindungstyp die Rolle des SSL-Clients oder des SSL-Servers.

In der folgenden Tabelle sind die Rollen des IMM bei sicheren Web-Server-Verbindungen und sicheren LDAP-Verbindungen dargestellt.

Tabelle 14. IMM-Unterstützung von SSL-Verbindungen

Verbindungstyp	SSL-Client	SSL-Server
Sicherer Web-Server (HTTPS)	Web-Browser (z. B. Microsoft Internet Explorer)	IMM-Web-Server
Sichere IBM Systems Director-Verbindung	IBM Systems Director	IMM Systems Director-Server
Sichere LDAP-Verbindung (LDAPS)	IMM-LDAP-Client	Ein LDAP-Server

Sie können die SSL-Einstellungen auf der Seite "Security" (Sicherheit) anzeigen oder ändern; dies umfasst das Aktivieren oder Inaktivieren von SSL und das Verwalten erforderlicher Zertifikate für SSL.

SSL-Zertifikat

Sie können SSL entweder mit einem selbst signierten Zertifikat oder mit einem von einer unabhängigen Zertifizierungsstelle signierten Zertifikat verwenden.

Ein selbst signiertes Zertifikat ist die einfachste Methode für die Verwendung von SSL, allerdings stellt es ein Sicherheitsrisiko dar. Wenn Sie diese Methode wählen, hat der SSL-Client keine Möglichkeit, beim ersten Verbindungsversuch zwischen Client und Server die Identität des SSL-Servers zu prüfen. Ein anderer Anbieter kann möglicherweise die Identität des Servers vortäuschen und Daten zwischen dem IMM und dem Web-Browser abfangen. Wenn das selbst signierte Zertifikat beim ersten Verbindungsaufbau zwischen dem Browser und dem IMM in den Zertifikatsspeicher des Browsers importiert wird, sind alle künftigen Datenübertragungen für diesen Browser sicher, vorausgesetzt, dass bei der ersten Verbindung kein Angriff erfolgt ist.

Mehr Sicherheit erhalten Sie, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert ist. Um ein signiertes Zertifikat zu erhalten, verwenden Sie die Seite zur Verwaltung von SSL-Zertifikaten, um eine Unterzeichnungsanforderung für ein SSL-Zertifikat zu erstellen. Senden Sie dann die Unterzeichnungsanforderung für das SSL-Zertifikat an eine Zertifizierungsstelle und vereinbaren Sie die Zustellung eines Zertifikats. Sobald Sie das Zertifikat erhalten haben, wird es über den Link **Import a Signed Certificate** (Signiertes Zertifikat importieren) in das IMM importiert und Sie können SSL aktivieren.

Die Aufgabe der Zertifizierungsstelle ist es, die Identität des IMM zu überprüfen. Ein Zertifikat enthält digitale Signaturen für die Zertifizierungsstelle und das IMM. Wenn eine anerkannte Zertifizierungsstelle das Zertifikat ausstellt oder wenn das Zertifikat der Zertifizierungsstelle bereits in den Web-Browser importiert wurde, kann der Browser das Zertifikat validieren und den Web-Server des IMM positiv identifizieren.

Das IMM benötigt ein Zertifikat für den sicheren Web-Server und eines für den sicheren LDAP-Client. Der sichere LDAP-Client benötigt ebenfalls ein oder mehrere vertrauenswürdige Zertifikate. Das vertrauenswürdige Zertifikat wird vom sicheren LDAP-Client verwendet, um den LDAP-Server sicher zu identifizieren. Das vertrauenswürdige Zertifikat ist das Zertifikat der Zertifizierungsstelle, die das Zertifikat des LDAP-Servers signiert hat. Wenn der LDAP-Server selbst signierte Zertifikate verwendet, kann das vertrauenswürdige Zertifikat das Zertifikat des LDAP-Servers selbst sein. Sie müssen zusätzliche vertrauenswürdige Zertifikate importieren, wenn Sie in Ihrer Konfiguration mehrere LDAP-Server verwenden.

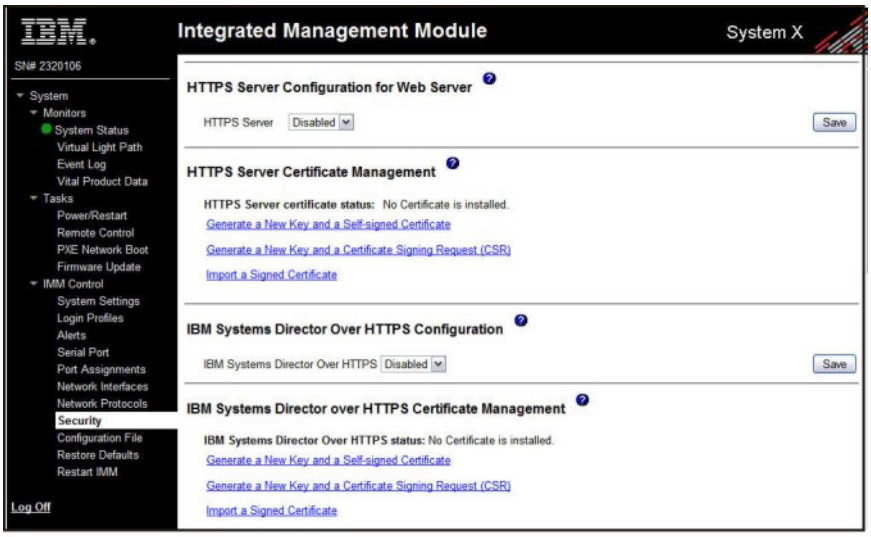
Verwaltung von SSL-Serverzertifikaten

Der SSL-Server erfordert, dass ein gültiges Zertifikat und ein entsprechender privater Chiffrierschlüssel installiert werden, bevor SSL aktiviert wird. Es stehen zwei Methoden zur Verfügung, um den privaten Schlüssel und das erforderliche Zertifikat zu generieren: Die Verwendung eines selbst signierten Zertifikats und die Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats. Weitere Informationen zur Verwendung eines selbst signierten Zertifikats für den SSL-Server finden Sie unter „Selbst signiertes Zertifikat erstellen". Weitere Informationen zur Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats für den SSL-Server finden Sie unter „Zertifikatssignieranforderung erstellen" auf Seite 94.

Selbst signiertes Zertifikat erstellen

Gehen Sie wie folgt vor, um einen neuen privaten Chiffrierschlüssel und ein selbst signiertes Zertifikat zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit). Die folgende Seite wird angezeigt.



2. Stellen Sie sicher, dass die Einstellung für den Bereich **SSL Server Configuration for Web Server** oder den Bereich **IBM Systems Director Over HTTPS Configuration** auf **Disabled** (Inaktiviert) gesetzt ist. Falls sie nicht inaktiviert ist, wählen Sie **Disabled** aus und klicken Sie anschließend auf **Save** (Speichern).

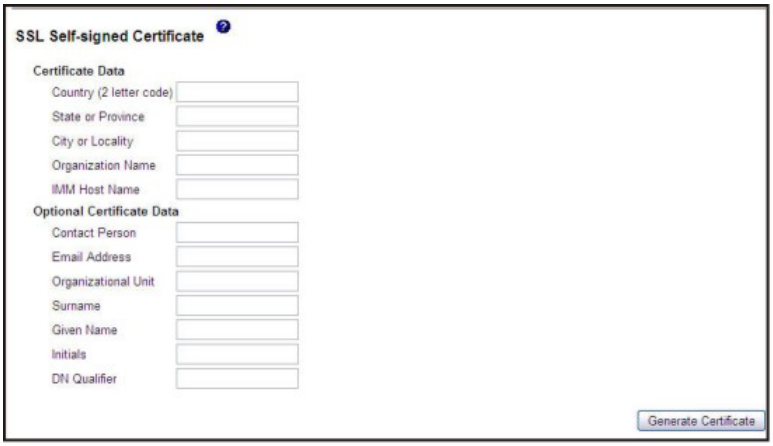
   Anmerkung:

   a. Das IMM muss erneut gestartet werden, damit der ausgewählte Wert (**Enabled** (Aktiviert) oder **Disabled**) wirksam wird.

   b. Damit SSL aktiviert werden kann, muss ein gültiges SSL-Zertifikat vorhanden sein.

   c. Zum Verwenden von SSL müssen Sie einen Client-Web-Browser für die Verwendung von SSL3 oder TLS konfigurieren. Browser älteren Exportgrades, die nur SSL2 unterstützen, können nicht verwendet werden.

3. Wählen Sie im Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) die Option **Generate a New Key and a Self-signed Certificate** (Neuen Schlüssel und selbst signiertes Zertifikat erstellen) aus. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



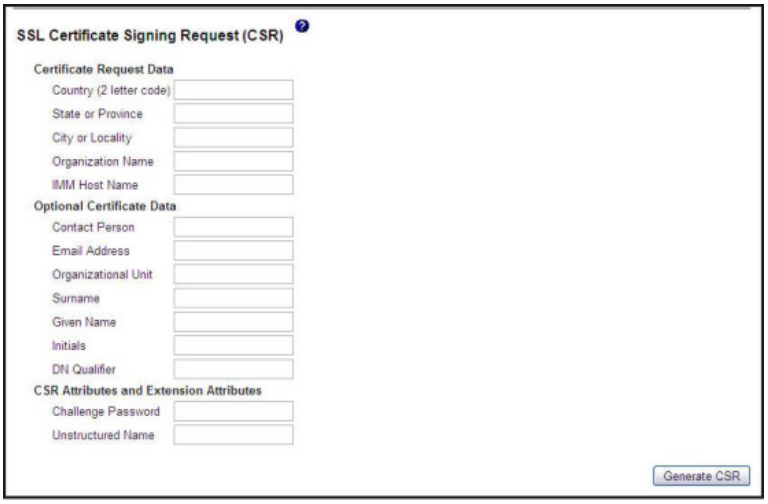
4. Geben Sie die Informationen in die erforderlichen und optionalen Felder zu Ihrer Konfiguration ein. Eine Beschreibung der Felder finden Sie unter “Required certificate data” (Erforderliche Zertifikatsdaten). 94. Nachdem Sie die Informati-

onen eingegeben haben, klicken Sie auf **Generate Certificate** (Zertifikat erstellen). Ihre neuen Chiffrierschlüssel und das Zertifikat werden erstellt. Dieser Vorgang kann einige Minuten dauern. Wenn ein selbst signiertes Zertifikat installiert wird, wird Ihnen eine Bestätigung angezeigt.

Zertifikatssignieranforderung erstellen

Gehen Sie wie folgt vor, um einen neuen privaten Chiffrierschlüssel und eine Zertifikatssignieranforderung zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Security**.
2. Stellen Sie im Bereich **SSL Server Configuration for Web Server** sicher, dass der SSL-Server inaktiviert ist. Falls er nicht inaktiviert ist, wählen Sie **Disabled** (Inaktiviert) im Feld **SSL Server** aus und klicken Sie anschließend auf **Save**.
3. Wählen Sie im Bereich **SSL Server Certificate Management** die Option **Generate a New Key and a Certificate-Signing Request** (Neuen Schlüssel und Zertifikatssignieranforderung generieren) aus. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



4. Geben Sie die Informationen in die erforderlichen und optionalen Felder zu Ihrer Konfiguration ein. Die Felder sind dieselben wie beim selbst signierten Zertifikat; ergänzend kommen noch einige Felder hinzu.

   Lesen Sie die Informationen in den folgenden Abschnitten, um eine Beschreibung jedes der allgemeinen Felder zu bekommen.

   Erforderliche Zertifikatsdaten Die folgenden Benutzereingabefelder sind erforderlich, um ein selbst signiertes Zertifikat oder eine Zertifikatssignieranforderung zu erstellen:

   Country (Land)
   Geben Sie in diesem Feld das Land an, in dem sich das IMM befindet. Dieses Feld muss den aus 2 Zeichen bestehenden Landescode enthalten.

   State or Province (Bundesland)
   Geben Sie in diesem Feld an, in welchem Staat oder in welcher Region sich das IMM befindet. Dieses Feld ist auf maximal 30 Zeichen begrenzt.

   City or Locality (Ort oder Standort)
   Geben Sie in diesem Feld an, in welcher Stadt oder in welchem Ort sich das IMM befindet. Dieses Feld ist auf maximal 50 Zeichen begrenzt.

Organization Name (Name des Unternehmens)
Geben Sie in diesem Feld an, welchem Unternehmen oder welcher Organisation das IMM gehört. Wenn diese Informationen zum Erstellen einer Zertifikatssignieranforderung verwendet werden, kann die ausstellende Zertifizierungsstelle überprüfen, ob das Unternehmen, das das Zertifikat anfordert, gesetzlich berechtigt ist, Eigentumsrechte am angegebenen Unternehmens- oder Organisationsnamen zu beanspruchen. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

IMM Host Name (Hostname des IMM)
Geben Sie in diesem Feld den Hostnamen des IMM an, der derzeit im Adressfeld des Web-Browsers angezeigt wird.

Achten Sie darauf, dass der Wert, den Sie in diesem Feld eingeben, exakt mit dem Hostnamen übereinstimmt, den der Web-Browser kennt. Der Browser vergleicht den Hostnamen in der angezeigten Webadresse mit dem Namen, der im Zertifikat steht. Um Zertifikatwarnungen vom Browser zu vermeiden, muss der in diesem Feld angegebene Wert mit dem Hostnamen übereinstimmen, der vom Browser zum Herstellen einer Verbindung mit dem IMM verwendet wird. Wenn die Adresse in der Webadressleiste beispielsweise "http://mm11.xyz.com/private/main.ssi" lautet, muss der im Feld "IMM Host Name" angegebene Wert "mm11.xyz.com" lauten. Wenn die Webadresse "http://mm11/private/main.ssi" lautet, muss der verwendete Wert "mm11" lauten. Wenn die Webadresse "http://192.168.70.2/private/main.ssi" lautet, muss der verwendete Wert "192.168.70.2" lauten.

Dieses Zertifikatattribut wird im Allgemeinen als "allgemeiner Name" bezeichnet.

Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Contact Person (Ansprechpartner)
Geben Sie in diesem Feld den Namen eines Ansprechpartners an, der für das IMM verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Email Address (E-Mail-Adresse)
Geben Sie in diesem Feld die E-Mail-Adresse eines Ansprechpartners an, der für das IMM verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Optionale Zertifikatsdaten Die folgenden Benutzereingabefelder sind bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung optional:

Organizational Unit (Organisationseinheit)
Geben Sie in diesem Feld die Einheit innerhalb des Unternehmens oder der Organisation an, der das IMM gehört. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Surname (Nachname)
Geben Sie in diesem Feld zusätzliche Informationen an, etwa den Nachnamen einer Person, die für das IMM verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Given Name (Vorname)
Geben Sie in diesem Feld zusätzliche Informationen an, etwa den Vornamen einer Person, die für das IMM verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Initials (Initialen)
Geben Sie in diesem Feld zusätzliche Informationen an, etwa die Initialen einer Person, die für das IMM verantwortlich ist. Dieses Feld ist auf maximal 20 Zeichen begrenzt.

DN Qualifier (Qualifikationsmerkmal eines definierten Namens)
Geben Sie in diesem Feld zusätzliche Informationen an, etwa das Qualifikationsmerkmal eines definierten Namens für das IMM. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Attribute einer Zertifikatssignieranforderung Die folgenden Felder sind optional, es sei denn, sie werden von der Zertifizierungsstelle benötigt, die Sie ausgewählt haben:

Challenge Password (Kennwort abfragen)
Verwenden Sie dieses Feld, um der Zertifikatssignieranforderung ein Kennwort zuzuweisen. Dieses Feld ist auf maximal 30 Zeichen begrenzt.

Unstructured Name (Unstrukturierter Name)
Geben Sie in diesem Feld zusätzliche Informationen an, etwa einen unstrukturierten Namen, der dem IMM zugewiesen ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

5. Nachdem Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Generate CSR** (Zertifikatssignieranforderung erstellen). Nun werden der neue Chiffrierschlüssel und das Zertifikat generiert. Dieser Vorgang kann einige Minuten dauern.
6. Klicken Sie auf **Download CSR** und dann auf **Save**, um die Datei auf Ihrer Workstation zu speichern. Beim Erstellen der Zertifikatssignieranforderung wird eine Datei im Format DER erstellt. Falls die Zertifizierungsstelle ein anderes Format verlangt, etwa PEM, können Sie die Datei mithilfe eines Tools wie OpenSSL umwandeln (http://www.openssl.org). Wenn Sie von Ihrer Zertifizierungsstelle aufgefordert werden, den Inhalt der Datei mit der Zertifikatssignieranforderung in ein Web-Browser-Fenster zu kopieren, wird in der Regel eine Datei im PEM-Format erwartet.

   Der Befehl zum Konvertieren einer Zertifikatssignieranforderung von DER in PEM mittels OpenSSL lautet ähnlich wie im folgenden Beispiel:

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```
7. Senden Sie die Zertifikatssignieranforderung an Ihre Zertifizierungsstelle. Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle zurückerhalten, müssen Sie es ggf. in das Format DER umwandeln. (Wenn Sie das Zertifikat als Text in einer E-Mail oder Webseite erhalten haben, ist es vermutlich im PEM-Format.) Sie können das Format mithilfe eines Tools, das von Ihrer Zertifizierungsstelle bereitgestellt wird, oder mithilfe eines Tools wie OpenSSL (http://www.openssl.org) ändern. Der Befehl zum Konvertieren eines Zertifikats von PEM in DER lautet ähnlich wie im folgenden Beispiel:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle zurückerhalten haben, fahren Sie mit Schritt 8 fort.
8. Klicken Sie im Navigationsfenster auf **Security**. Blättern Sie zum Bereich **SSL Server Certificate Management** oder zum Bereich **IBM Systems Director Over HTTPS Certificate Management**.
9. Klicken Sie auf **Import a Signed Certificate** (Signiertes Zertifikat importieren).
10. Klicken Sie auf **Browse** (Durchsuchen).
11. Klicken Sie auf die gewünschte Zertifikatsdatei und dann auf **Open**. Der Dateiname (mit Angabe des vollständigen Pfads) wird in dem Feld neben der Schaltfläche **Browse** angezeigt.
12. Klicken Sie auf **Import Server Certificate** (Serverzertifikat importieren), um den Vorgang zu starten. Während die Datei auf den Speicher des IMM übertragen wird, wird eine Statusanzeige angezeigt. Zeigen Sie diese Seite solange an, bis die Übertragung abgeschlossen ist.

SSL für den sicheren Web-Server oder IBM Systems Director über HTTPS aktivieren

Gehen Sie wie folgt vor, um den sicheren Web-Server zu aktivieren.

Anmerkung: Damit SSL aktiviert werden kann, muss ein gültiges SSL-Zertifikat installiert werden.

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit). Die Seite, die angezeigt wird, zeigt, dass ein gültiges SSL-Serverzertifikat installiert wurde. Wenn der Status des SSL-Serverzertifikats nicht angibt, dass ein gültiges SSL-Zertifikat installiert wurde, lesen Sie die Informationen im Abschnitt „Verwaltung von SSL-Serverzertifikaten" auf Seite 92.
2. Blättern Sie abwärts bis zum Bereich **SSL Server Configuration for web Server** (Konfiguration des SSL-Servers für den Web-Server) oder bis zum Bereich **IBM Systems Director Over HTTPS Configuration** (Konfiguration von IBM Systems Director über HTTPS), wählen Sie **Enabled** (Aktiviert) im Feld **SSL Client** aus und klicken Sie auf **Save** (Speichern). Der ausgewählte Wert wird nach dem nächsten Neustart des IMM wirksam.

Verwaltung von SSL-Clientzertifikaten

Der SSL-Client erfordert, dass ein gültiges Zertifikat und ein entsprechender privater Chiffrierschlüssel installiert werden, bevor SSL aktiviert wird. Es sind zwei Methoden zum Generieren des privaten Schlüssels und des erforderlichen Zertifikats verfügbar: Sie können ein selbst signiertes Zertifikat oder ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden.

Die Vorgehensweise zum Erstellen des privaten Chiffrierschlüssels und Zertifikats für den SSL-Client ist dieselbe wie beim SSL-Server, nur dass Sie nicht den Bereich **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) auf der Webseite "Security" (Sicherheit) verwenden, sondern den Bereich **SSL Client Certificate Management** (Verwaltung von SSL-Clientzertifikaten). Informationen zur Verwendung eines selbst signierten Zertifikat für den SSL-Client finden Sie im Abschnitt „Selbst signiertes Zertifikat erstellen" auf Seite 92. Weitere Informationen zur Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats für den SSL-Client finden Sie unter „Zertifikatssignieranforderung erstellen" auf Seite 94.

Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten

Der sichere SSL-Client (LDAP-Client) verwendet vertrauenswürdige Zertifikate, um den LDAP-Server positiv zu identifizieren. Ein vertrauenswürdiges Zertifikat kann das Zertifikat der Zertifizierungsstelle sein, die das Zertifikat des LDAP-Servers signiert hat, oder es kann das Zertifikat des LDAP-Servers selbst sein. Bevor der SSL-Client aktiviert wird, muss mindestens ein Zertifikat in das IMM importiert werden. Sie können bis zu drei vertrauenswürdige Zertifikate importieren.

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat zu importieren:

1. Wählen Sie im Navigationsfenster die Option **Security** aus.
2. Stellen Sie im Bereich **SSL Client Configuration for LDAP Client** sicher, dass der SSL-Client inaktiviert ist. Falls er nicht inaktiviert ist, wählen Sie **Disabled** (Inaktiviert) im Feld **SSL Client** aus und klicken Sie anschließend auf **Save**.
3. Blättern Sie zum Bereich **SSL Client Trusted Certificate Management**) (SSL-Client-Verwaltung von vertrauenswürdigen Zertifikaten).
4. Klicken Sie neben einem der Felder **Trusted CA Certificate 1** (Zertifikat 1 einer vertrauenswürdigen Zertifizierungsstelle) auf **Import**.

5. Klicken Sie auf **Browse** (Durchsuchen).
6. Wählen Sie die gewünschte Zertifikatsdatei aus und klicken Sie auf **Open**. Der Dateiname wird unter Angabe des vollständigen Pfads im Feld neben der Schaltfläche **Browse** angezeigt.
7. Zum Starten des Importprozesses klicken Sie auf **Import Certificate** (Zertifikat importieren). Während die Datei auf den Speicher des IMM übertragen wird, wird eine Statusanzeige angezeigt. Zeigen Sie diese Seite solange an, bis die Übertragung abgeschlossen ist.

   Nun steht die Schaltfläche **Remove** (Entfernen) für die Option "Trusted CA Certificate 1" zur Verfügung. Wenn Sie ein vertrauenswürdiges Zertifikat entfernen möchten, klicken Sie auf die entsprechende Schaltfläche **Remove**.

   Mithilfe der jeweiligen Schaltfläche **Import** neben "Trusted CA Certificate 2" und "Trusted CA Certificate 3" können Sie weitere vertrauenswürdige Zertifikate importieren.

SSL für den LDAP-Client aktivieren

Verwenden Sie den Bereich **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client) der Seite "Security" (Sicherheit), um SSL für den LDAP-Client zu aktivieren oder zu inaktivieren. Um SSL aktivieren zu können, müssen Sie zuerst ein gültiges SSL-Clientzertifikat und mindestens ein vertrauenswürdiges Zertifikat installieren.

Gehen Sie wie folgt vor, um SSL für den Client zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit).

   Auf der Seite "Security" werden ein installiertes SSL-Clientzertifikat und das vertrauenswürdige Zertifikat 1 einer Zertifizierungsstelle angezeigt.
2. Wählen Sie auf der Seite "SSL Client Configuration for LDAP Client´" (Konfiguration des SSL-Clients für den LDAP-Client) im Feld **SSL Client** (SSL-Client) die Option **Enabled** (Aktiviert) aus.

   Anmerkung:

   a. Der ausgewählte Wert ("Enabled" (Aktiviert) bzw. "Disabled" (Inaktiviert)) wird sofort wirksam.
   b. Damit SSL aktiviert werden kann, muss ein gültiges SSL-Zertifikat vorhanden sein.
   c. Ihr LDAP-Server muss SSL3 oder TLS unterstützen, damit er kompatibel mit der SSL-Implementierung ist, die der LDAP-Client verwendet.
3. Klicken Sie auf **Save** (Speichern). Der ausgewählte Wert wird sofort wirksam.

Verschlüsselungsverwaltung

Verwenden Sie den Bereich **Cryptography Management** (Verschlüsselungsverwaltung) der Seite "Security" (Sicherheit), um die Stärke der Cipher-Suites für SSL-Server im IMM einschließlich des HTTPS-Servers und IBM System Director über HTTPS zu konfigurieren.

Die Verschlüsselungsverwaltungsmodi haben unterschiedliche Sicherheitsstärken. Der Modus "Basic Compatible" ist der Standardmodus und ist mit älteren Firmwareversionen sowie mit Browsern und anderen Netzclients kompatibel, auf denen die strengeren Sicherheitsanforderungen nicht implementiert werden. Beim Modus "High Security" (Hohe Sicherheit) darf das IMM nur einen symmetrischen SSL-Schlüssel mit einer Länge von mindestens 128 Bit verwenden.

Gehen Sie wie folgt vor, um den Modus zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit).
2. Suchen Sie den Bereich **Cryptography Management** (Verschlüsselungsverwaltung) und wählen Sie den Modus **Basic Compatible Mode** (Basiskompatibilitätsmodus) oder **High Security Mode** (Hochsicherheitsmodus) aus.
3. Klicken Sie auf **Save** (Speichern); der ausgewählte Modus wird dadurch nach einem Neustart des IMM wirksam.

Secure Shell-Server konfigurieren

Die SSH-Funktion (Secure Shell) ermöglicht den sicheren Zugriff auf die Befehlszeilenschnittstelle und die seriellen Umleitungsfunktionen (Textkonsole) des IMM.

Secure Shell-Benutzer werden durch den Austausch von Benutzer-ID und Kennwort authentifiziert. Das Kennwort und die Benutzer-ID werden gesendet, nachdem der Verschlüsselungskanal erstellt wurde. Das aus Benutzer-ID und Kennwort bestehende Paar kann eines der 12 lokal gespeicherten Paare bestehend aus Benutzer-ID und Kennwort sein oder auf einem LDAP-Server gespeichert werden. Eine Authentifizierung über öffentlichen Schlüssel wird nicht unterstützt.

Secure Shell-Serverschlüssel generieren

Mit einem Secure Shell-Serverschlüssel wird die Identität des Secure Shell-Servers dem Client gegenüber authentifiziert. Secure Shell muss inaktiviert sein, bevor Sie einen neuen privaten Secure Shell-Serverschlüssel erstellen können. Sie müssen zuerst einen Serverschlüssel erstellen, bevor Sie den Secure Shell-Server aktivieren.

Wenn Sie einen neuen Serverschlüssel anfordern, werden gleichzeitig ein Rivest-, ein Shamir- und ein Adelman- sowie ein DSA-Schlüssel erstellt, um den Zugang zum IMM eines Client für SSH-Version 2 zu ermöglichen. Aus Sicherheitsgründen wird der private Secure Shell-Schlüssel beim Speichern oder Wiederherstellen der Konfiguration nicht gesichert.

Gehen Sie wie folgt vor, um einen neuen Secure Shell-Schlüssel zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Security**.
2. Blättern Sie zum Bereich **Secure Shell (SSH) Server** und stellen Sie sicher, dass der Secure Shell-Server inaktiviert ist. Wenn er nicht inaktiviert ist, wählen Sie im Feld **SSH Server Disabled** (Inaktiviert) aus und klicken Sie dann auf **Save**.
3. Blättern Sie zum Bereich **SSH Server Key Management** (SSH-Serverschlüsselverwaltung).
4. Klicken Sie auf **Generate SSH Server Private Key** (Privaten SSH-Serverschlüssel erstellen). Ein Statusfenster wird geöffnet. Warten Sie, bis der Vorgang abgeschlossen ist.

Secure Shell-Server aktivieren

Auf der Seite "Security" (Sicherheit) können Sie den Secure Shell-Server aktivieren oder inaktivieren. Die Auswahl, die Sie hier treffen, wird erst nach einem Neustart des IMM wirksam. Der Wert, der in der Anzeige erscheint ("Enabled" (Aktiviert) oder "Disabled" (Inaktiviert)), ist der zuletzt ausgewählte Wert und der Wert, der beim Neustart des IMM verwendet wird.

Anmerkung: Der Secure Shell-Server kann nur aktiviert werden, wenn ein gültiger privater Schlüssel für den Secure Shell-Server installiert ist.

Gehen Sie wie folgt vor, um den Secure Shell-Server zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit).
2. Blättern Sie abwärts bis zum Abschnitt **Secure Shell (SSH) Server**.
3. Klicken Sie im Feld **SSH Server** (SSH-Server) auf **Enabled** (Aktiviert).
4. Klicken Sie im Navigationsfenster auf **Restart IMM**, um das IMM erneut zu starten.

Secure Shell-Server verwenden

Wenn Sie den im Lieferumfang von Red Hat Linux, Version 7.3, enthaltenen SSH-Client verwenden, um eine Secure Shell-Sitzung mit einem IMM mit der Netzadresse 192.168.70.132 zu starten, geben Sie einen dem folgenden Beispiel ähnlichen Befehl ein:

```
ssh -x -l userid 192.168.70.132.
```

Dabei gibt "-x" an, dass keine X Window System-Weiterleitung erfolgt, und "-l" gibt an, dass die Sitzung die Benutzer-ID *userid* verwenden soll.

Ihre IMM-Konfiguration wiederherstellen und ändern

Sie können eine gespeicherte Konfiguration vollständig wiederherstellen oder Sie können Schlüsselfelder der gespeicherten Konfiguration ändern, bevor Sie die Konfiguration auf Ihrem IMM wiederherstellen. Indem Sie die Konfigurationsdatei vor der Wiederherstellung ändern, können Sie mehrere IMMs mit ähnlichen Konfigurationen einrichten. Sie können schnell Parameter wie etwa Namen und IP-Adressen angeben, die eindeutige Werte erfordern, ohne allgemein freigegebene Informationen eingeben zu müssen.

Gehen Sie wie folgt vor, um Ihre aktuelle Konfiguration wiederherzustellen oder zu ändern:

1. Melden Sie sich an dem IMM an, dessen Konfiguration Sie wiederherstellen möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Configuration File** (Konfigurationsdatei).
3. Klicken Sie im Bereich **Restore IMM Configuration** (IMM-Konfiguration wiederherstellen) auf **Browse** (Durchsuchen).
4. Klicken Sie auf die gewünschte Konfigurationsdatei und dann auf **Open**. Die Datei (samt vollständigem Pfad) wird im Feld neben der Schaltfläche **Browse** angezeigt.
5. Wenn Sie keine Änderungen an der Konfigurationsdatei vornehmen möchten, klicken Sie auf **Restore** (Wiederherstellen). Ein neues Fenster mit den IMM-Konfigurationsdaten wird geöffnet. Stellen Sie sicher, dass es sich um die Konfiguration handelt, die Sie wiederherstellen möchten. Handelt es sich nicht um die richtige Konfiguration, klicken Sie auf **Cancel** (Abbrechen).

   Wenn Sie die Konfigurationsdatei ändern möchten, bevor Sie die Konfiguration wiederherstellen, klicken Sie auf **Modify and Restore** (Ändern und wiederherstellen), um so ein Fenster mit einer editierbaren Konfigurationszusammenfassung zu öffnen. Zunächst werden nur die Felder angezeigt, die Sie ändern können. Um von dieser Ansicht auf die Ansicht der vollständigen Konfigurationszusammenfassung zu wechseln, klicken Sie auf die Schaltfläche **Toggle View** (Ansicht umschalten) oben oder unten im Fenster. Klicken Sie zum Ändern des Inhalts eines Feldes auf das entsprechende Textfeld und geben Sie die Daten ein.

Anmerkung: Wenn Sie auf **Restore** (Wiederherstellen) oder auf **Modify and Restore** klicken, wird möglicherweise ein Alertfenster geöffnet, wenn die Konfigurationsdatei, die Sie wiederherzustellen versuchen, mit einem anderen Serviceprozessortyp oder dem gleichen Serviceprozessortyp mit älterer Firmware (und daher mit weniger Funktionalität) erstellt wurde.
Diese Alertnachricht enthält eine Liste mit Systemverwaltungsfunktionen, die Sie nach beendeter Wiederherstellung konfigurieren müssen. Einige Funktionen erfordern Konfigurationen in mehr als einem Fenster.

6. Klicken Sie auf **Restore Configuration** (Konfiguration wiederherstellen), um mit dem Wiederherstellen dieser Datei auf dem IMM fortzufahren. Während der Aktualisierung der Firmware auf dem IMM wird eine Statusanzeige geöffnet. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

   Anmerkung: Die Sicherheitseinstellungen auf der Seite "Security" werden bei der Wiederherstellungsoperation nicht wiederhergestellt. Informationen zum Verändern von Sicherheitseinstellungen finden Sie im Abschnitt „Web-Server, IBM Systems Director und sichere LDAP-Verbindung sichern" auf Seite 91.
7. Klicken Sie nach Erhalt einer Bestätigung, dass der Wiederherstellungsprozess abgeschlossen ist, im Navigationsfenster auf **Restart IMM** und dann auf **Restart**.
8. Klicken Sie auf **OK**, um zu bestätigen, dass Sie das IMM erneut starten möchten.
9. Klicken Sie auf **OK**, um das aktuelle Browserfenster zu schließen.
10. Um sich erneut am IMM anzumelden, starten Sie den Browser und führen Sie den Anmeldeprozess wie üblich durch.

Konfigurationsdatei verwenden

Wählen Sie im Navigationsfenster **Configuration File** (Konfigurationsdatei) aus, um die IMM-Konfiguration zu sichern und wiederherzustellen.

Wichtig: Einstellungen der Seite "Security" werden bei der Sicherung nicht gespeichert und können bei der Wiederherstellung nicht wiederhergestellt werden.

Aktuelle Konfiguration sichern

Sie können eine Kopie Ihrer aktuellen IMM-Konfiguration auf den Client-Computer herunterladen, auf dem die IMM-Webschnittstelle ausgeführt wird. Mithilfe dieser Sicherungskopie können Sie die IMM-Konfiguration wiederherstellen, wenn sie versehentlich geändert oder beschädigt wurde. Verwenden Sie diese Sicherungskopie als Basis, die Sie ändern können, um mehrere IMMs mit ähnlicher Konfiguration zu konfigurieren.

Die Konfigurationsdaten, die bei dieser Prozedur gespeichert werden, schließen nicht die Konfigurationseinstellungen für die System x Server-Firmware oder die IPMI-Einstellungen ein, die von dem Nicht-IMPI-Benutzerschnittstellen abweichen.

Gehen Sie wie folgt vor, um die aktuelle Konfiguration zu sichern:

1. Melden Sie sich an dem IMM an, dessen aktuelle Konfiguration Sie sichern möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Configuration File** (Konfigurationsdatei).

3. Klicken Sie im Bereich **Backup IMM Configuration** (IMM-Konfiguration sichern) auf **View the current configuration summary** (Zusammenfassung zur aktuellen Konfiguration anzeigen).
4. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Close** (Schließen).
5. Um diese Konfiguration zu sichern, klicken Sie auf **Backup** (Sichern).
6. Geben Sie einen Namen für die Sicherungskopie ein, wählen Sie den Speicherort für die Datei aus und klicken Sie auf **Save** (Speichern).

   Klicken Sie in Mozilla Firefox auf **Save File** (Datei speichern) und dann auf **OK**.

   Klicken Sie in Microsoft Internet Explorer auf **Datei auf Datenträger speichern** und dann auf **OK**.

Ihre IMM-Konfiguration wiederherstellen und ändern

Sie können eine gespeicherte Konfiguration vollständig wiederherstellen oder Sie können Schlüsselfelder der gespeicherten Konfiguration ändern, bevor Sie die Konfiguration auf Ihrem IMM wiederherstellen. Indem Sie die Konfigurationsdatei vor der Wiederherstellung ändern, können Sie mehrere IMMs mit ähnlichen Konfigurationen einrichten. Sie können schnell Parameter wie etwa Namen und IP-Adressen angeben, die eindeutige Werte erfordern, ohne allgemein freigegebene Informationen eingeben zu müssen.

Gehen Sie wie folgt vor, um Ihre aktuelle Konfiguration wiederherzustellen oder zu ändern:

1. Melden Sie sich an dem IMM an, dessen Konfiguration Sie wiederherstellen möchten. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Configuration File** (Konfigurationsdatei).
3. Klicken Sie im Bereich **Restore IMM Configuration** (IMM-Konfiguration wiederherstellen) auf **Browse** (Durchsuchen).
4. Klicken Sie auf die gewünschte Konfigurationsdatei und dann auf **Open**. Die Datei (samt vollständigem Pfad) wird im Feld neben der Schaltfläche **Browse** angezeigt.
5. Wenn Sie keine Änderungen an der Konfigurationsdatei vornehmen möchten, klicken Sie auf **Restore** (Wiederherstellen). Ein neues Fenster mit den IMM-Konfigurationsdaten wird geöffnet. Stellen Sie sicher, dass es sich um die Konfiguration handelt, die Sie wiederherstellen möchten. Handelt es sich nicht um die richtige Konfiguration, klicken Sie auf **Cancel** (Abbrechen).

   Wenn Sie die Konfigurationsdatei ändern möchten, bevor Sie die Konfiguration wiederherstellen, klicken Sie auf **Modify and Restore** (Ändern und wiederherstellen), um so ein Fenster mit einer editierbaren Konfigurationszusammenfassung zu öffnen. Zunächst werden nur die Felder angezeigt, die Sie ändern können. Um von dieser Ansicht auf die Ansicht der vollständigen Konfigurationszusammenfassung zu wechseln, klicken Sie auf die Schaltfläche **Toggle View** (Ansicht umschalten) oben oder unten im Fenster. Klicken Sie zum Ändern des Inhalts eines Feldes auf das entsprechende Textfeld und geben Sie die Daten ein.

   Anmerkung: Wenn Sie auf **Restore** (Wiederherstellen) oder auf **Modify and Restore** klicken, wird möglicherweise ein Alertfenster geöffnet, wenn die Konfigurationsdatei, die Sie wiederherzustellen versuchen, mit einem anderen Serviceprozessortyp oder dem gleichen Serviceprozessortyp mit älterer Firmware (und daher mit weniger Funktionalität) erstellt wurde. Diese Alertnach-

richt enthält eine Liste mit Systemverwaltungsfunktionen, die Sie nach beendeter Wiederherstellung konfigurieren müssen. Einige Funktionen erfordern Konfigurationen in mehr als einem Fenster.

6. Klicken Sie auf **Restore Configuration** (Konfiguration wiederherstellen), um mit dem Wiederherstellen dieser Datei auf dem IMM fortzufahren. Während der Aktualisierung der Firmware auf dem IMM wird eine Statusanzeige geöffnet. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

   Anmerkung: Die Sicherheitseinstellungen auf der Seite "Security" werden bei der Wiederherstellungsoperation nicht wiederhergestellt. Informationen zum Verändern von Sicherheitseinstellungen finden Sie im Abschnitt „Web-Server, IBM Systems Director und sichere LDAP-Verbindung sichern" auf Seite 91.
7. Klicken Sie nach Erhalt einer Bestätigung, dass der Wiederherstellungsprozess abgeschlossen ist, im Navigationsfenster auf **Restart IMM** und dann auf **Restart**.
8. Klicken Sie auf **OK**, um zu bestätigen, dass Sie das IMM erneut starten möchten.
9. Klicken Sie auf **OK**, um das aktuelle Browserfenster zu schließen.
10. Um sich erneut am IMM anzumelden, starten Sie den Browser und führen Sie den Anmeldeprozess wie üblich durch.

Standardwerte wiederherstellen

Verwenden Sie, sofern Sie Administratorzugriff haben, den Link **Restore Defaults** (Standardwerte wiederherstellen), um die Standardkonfiguration des IMM wiederherzustellen.

Achtung: Wenn Sie auf **Restore Defaults** klicken, verlieren Sie sämtliche Änderungen, die Sie am IMM vorgenommen haben.

Gehen Sie wie folgt vor, um die IMM-Standardeinstellungen wiederherzustellen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Restore Defaults**, um die IMM-Standardeinstellungen wiederherzustellen. Wenn es sich um einen lokalen Server handelt, wird Ihre TCP/IP-Verbindung unterbrochen und Sie müssen die Netzschnittstelle rekonfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.
3. Melden Sie sich erneut an, um die IMM-Webschnittstelle zu verwenden.
4. Rekonfigurieren Sie die Netzschnittstelle, um wieder eine funktionsfähige Verbindung herzustellen. Informationen zur Netzschnittstelle finden Sie im Abschnitt „Netzschnittstellen konfigurieren" auf Seite 41.

IMM erneut starten

Verwenden Sie den Link **Restart IMM**, um das IMM erneut zu starten. Sie können diese Funktion nur ausführen, wenn Sie Administratorzugriff haben. Alle Ethernet-Verbindungen werden vorübergehend abgebrochen. Sie müssen sich erneut anmelden, um die IMM-Webschnittstelle zu verwenden.

Gehen Sie wie folgt vor, um das IMM erneut zu starten:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Restart IMM**, um das IMM erneut zu starten. Ihre TCP/IP- oder Modemverbindungen werden unterbrochen.
3. Melden Sie sich erneut an, um die IMM-Webschnittstelle zu verwenden.

Skalierbare Partitionierung

Das IMM ermöglicht es Ihnen, das System in einem skalierbaren Komplex zu konfigurieren und zu steuern.

Das IMM ermöglicht es Ihnen, das System in einem skalierbaren Komplex zu konfigurieren und zu steuern. Wenn auf dem Server ein Fehler auftritt, gibt das IMM einen Ereigniscode in die Ereignisprotokolle aus (siehe dazu „Ereignisprotokolle anzeigen” auf Seite 116).

1. Melden Sie sich an dem IMM an, dessen Konfiguration Sie wiederherstellen möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Scalable Partitioning** (Skalierbare Partitionierung) und klicken Sie anschließend auf **Manage Partitions** (Partitionen verwalten).

Funktion "Service Advisor"

Die Funktion "Service Advisor" erkennt und erfasst Systemhardwarefehlerereignisse und leitet die Daten automatisch zur Fehlerbestimmung an IBM Support weiter. Die Funktion "Service Advisor" kann außerdem Daten zu Systemfehler erfassen und diese Daten an IBM Support weiterleiten. Informationen dazu, ob Ihr Server diese Funktion unterstützt, finden Sie in der Dokumentation zu Ihrem Server. Die folgenden Abschnitte enthalten Anweisungen zum Konfigurieren, Testen und Warten von Service Advisor.

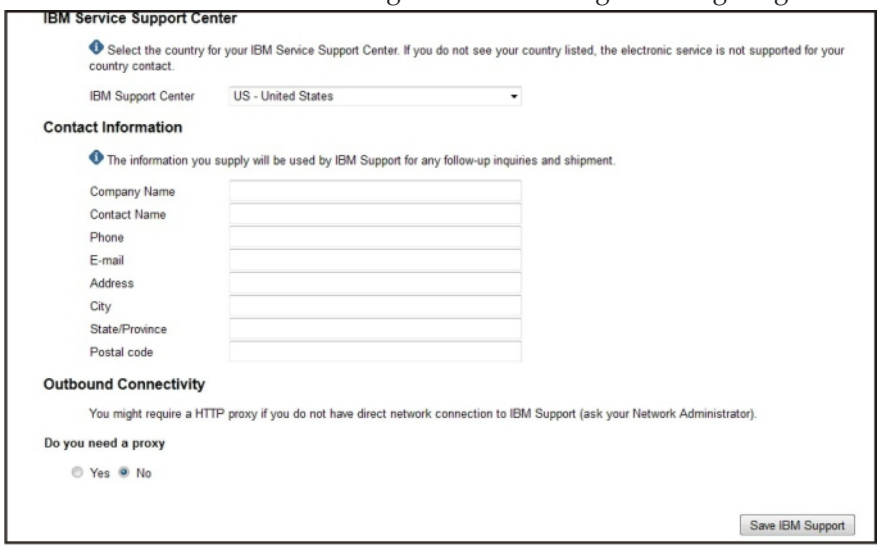
- Service Advisor konfigurieren
- Service Advisor verwenden

Service Advisor konfigurieren

Gehen Sie wie folgt vor, um Service Advisor zu konfigurieren:

1. Melden Sie sich an dem IMM an, für das Sie Service Advisor aktivieren möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden”, auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Service Advisor**.
3. Wenn Sie diese Option zum ersten Mal verwenden oder wenn das IMM auf die Standardwerte zurückgesetzt wurde, müssen Sie die Lizenzvereinbarung lesen und akzeptieren.
   a. Klicken Sie auf **View terms and conditions** (Nutzungsbedingungen anzeigen), um die Vereinbarung für Service Advisor anzuzeigen.
   b. Klicken Sie auf der Seite "Terms and Conditions" auf **I accept the agreement** (Ich akzeptiere die Vereinbarung), um Service Advisor zu aktivieren.
4. Klicken Sie auf die Registerkarte **Service Advisor Settings** (Einstellungen für Service Advisor).

Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



5. Geben Sie die Kontaktinformationen für den Serveradministrator ein. Die folgende Tabelle enthält Erläuterungen zu den Feldern für **Contact Information**.

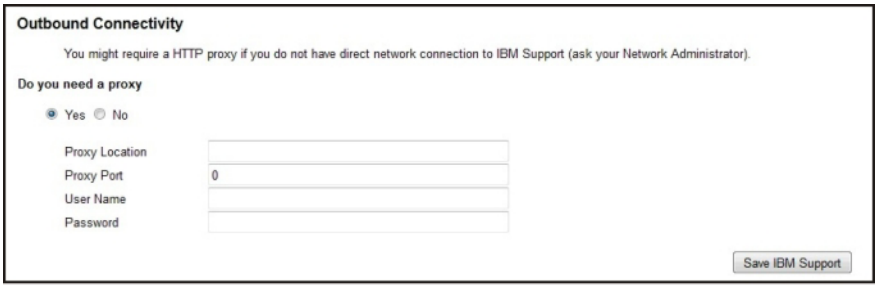
Tabelle 15. Kontaktinformationen

Feld	Beschreibung
IBM Service Support Center (IBM Service Support Center)	Geben Sie in diesem Feld den Landescode für das IBM Service Support Center an. Dies ist ein ISO-Landescode, der aus zwei Zeichen besteht. Er gilt nur für die Personen, die Zugriff auf das IBM Service Support Center haben.
Company Name (Name des Unternehmens)	Geben Sie in diesem Feld den Namen der Organisation oder des Unternehmens des Ansprechpartners an. Dieses Feld kann 1 bis 30 Zeichen enthalten.
Contact Name (Name des Ansprechpartners)	Geben Sie in diesem Feld den Namen der Organisation oder des Unternehmens des Ansprechpartners an. Dieses Feld kann 1 bis 30 Zeichen enthalten.
Phone (Telefon)	Geben Sie in diesem Feld die Telefonnummer des Ansprechpartners an. Dieses Feld kann 5 bis 30 Zeichen enthalten.
Email (E-Mail-Adresse)	Geben Sie in diesem Feld die E-Mail-Adresse des Ansprechpartners an. Die maximale Länge dieses Felds beträgt 30 Zeichen.
Address (Adresse)	Geben Sie in diesem Feld die Straße und Hausnummer an, in der sich das IMM physisch befindet. Dieses Feld kann 1 bis 30 Zeichen enthalten.
City (Ort)	Geben Sie in diesem Feld die Stadt oder den Ort an, in der sich das IMM physisch befindet.
State/Province (Bundesland)	Geben Sie in diesem Feld das Bundesland an, in dem sich das IMM physisch befindet. Dieses Feld kann 2 bis 3 Zeichen enthalten.
Postal Code (Postleitzahl)	Geben Sie in diesem Feld die Postleitzahl des Standorts für diesen Server an. Dieses Feld kann 1 bis 9 Zeichen enthalten (nur alphanumerische Zeichen sind gültig).

6. Erstellen Sie einen HTTP-Proxy, wenn das IMM keine direkte Netzverbindung zum IBM Support hat. Gehen Sie wie folgt vor, um die Konnektivitätsinformationen für abgehende Verbindungen zu konfigurieren.

a. Klicken Sie im Feld **Do you need a proxy** (Ist ein Proxy erforderlich) auf **Yes**. Weitere Informationen dazu enthält die vorherige Abbildung.

   Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

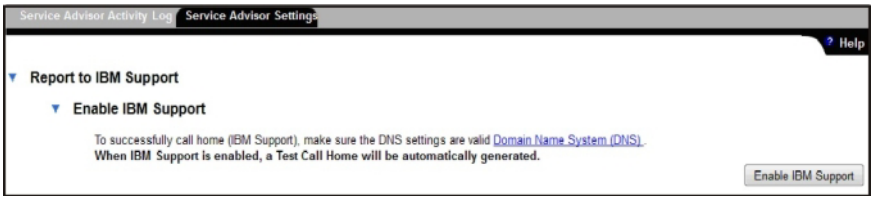


b. Geben Sie die entsprechenden Informationen unter **Proxy Location** (Proxy-Standort), **Proxy Port** (Proxy-Port), **User Name** (Benutzername) und **Password** (Kennwort) ein.

7. Klicken Sie auf **Save IBM Support**, um Ihre Änderungen zu speichern.
8. Klicken Sie auf **Enable IBM Support** (IBM Support aktivieren) (oben auf der Seite), um Service Advisor zu ermöglichen, IBM Support zu kontaktieren, wenn ein wartungsfähiger Ereigniscode generiert wurde.

   Anmerkung: Nachdem Sie IBM Support aktiviert haben, wird ein Testcode an die IBM Support-Site gesendet.
9. Klicken Sie auf die Registerkarte **Service Advisor Activity Log** (Aktivitätenprotokoll von Service Advisor), um den Status des Testcodes anzuzeigen.

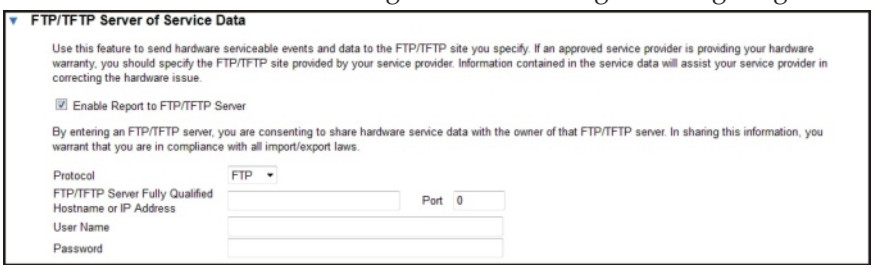
   Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



10. Wenn ein anderer Service-Provider die Ereigniscodes erhalten soll, bevor Sie IBM Support kontaktieren, klicken Sie auf **Enable Report to FTP/TFTP Server** (Bericht an FTP-/TFTP-Server aktivieren).

    Achtung: Indem Sie einen FTP-/TFTP-Server angeben, stimmen Sie zu, Hardware-Servicedaten für den Eigentümer dieses FTP-/TFTP-Servers freizugeben. Wenn Sie diese Informationen freigeben, gewährleisten Sie, dass Sie sich konform mit allen Import-/Exportgesetzen verhalten.

    Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



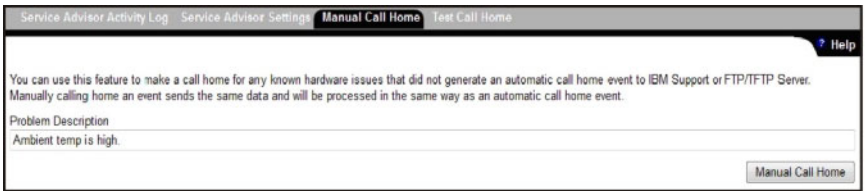
Service Advisor verwenden

Nach dem Konfigurieren des Service Advisor können Sie das Aktivitätenprotokoll anzeigen oder eine Testnachricht generieren.

Gehen Sie wie folgt vor, um einen Hardwarefehlerbericht für Ihren Server zu erstellen:

1. Melden Sie sich an dem IMM an, für das Sie Service Advisor verwenden möchten. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Service Advisor**.
3. Klicken Sie auf die Registerkarte **Manual Call Home** (Manuelle Call-Home-Funktion).

   Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

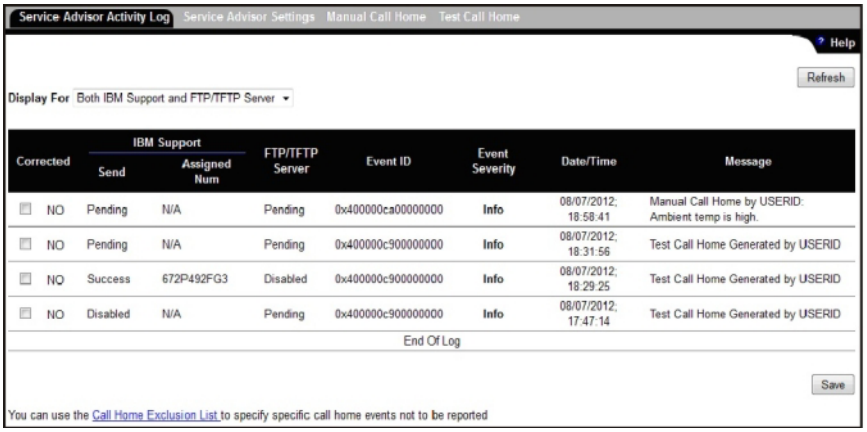


4. Gehen Sie wie folgt vor, um für ein Ereignis manuell eine Call-Home-Funktion auszuführen.
   a. Geben Sie die Fehlerbeschreibung in das Feld **Problem Description** ein.
   b. Klicken Sie auf die Schaltfläche **Manual Call Home** (Manuelle Call-Home-Funktion).
5. Zum Generieren einer Testnachricht klicken Sie auf die Registerkarte **Test Call Home** (Call-Home-Funktion testen) und wählen Sie dann die Schaltfläche **Test Call Home** (Call-Home-Funktion testen) aus.

   Anmerkungen:

   - Das Menü zum Testen der Call-Home-Funktion prüft den Kommunikationspfad zwischen dem IMM und IBM oder dem FTP-/TFTP-Server mit den aktuellen Einstellungen.
   - Wenn der Test nicht erfolgreich ist, überprüfen Sie die Netzkonfiguration.
   - Um einen Bericht für IBM Support zu erstellen, ist für Service Advisor die ordnungsgemäße Konfiguration der DNS-Serveradresse auf dem IMM erforderlich.
   - Ist das Senden erfolgreich, wird eine Servicenummer (Assigned Service Number) bzw. Ticketnummer zugewiesen. Das bei IBM Support geöffnete Ticket wird als Testticket gekennzeichnet. Für ein Testticket muss IBM Support keine Aktion durchführen, sodass der Aufruf geschlossen wird.
6. Klicken Sie auf die Registerkarte **Service Advisor Activity Log** (Aktivitätenprotokoll von Service Advisor), um den Status des Aktivitätenprotokolls anzuzeigen.

Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



Anmerkungen:

- Im Aktivitätenprotokoll werden die 5 neuesten Call-Home-Ereignisse angezeigt, darunter auch die Ereignisse, die sich auf Tests der Call-Home-Funktion und auf die manuelle Call-Home-Funktion beziehen.
- Die Ergebnisse im Feld **Send** können wie folgt aussehen:

  Success (Erfolgreich)
  Der Aufruf wurde erfolgreich bei IBM oder FTP/TFTP empfangen. Im Feld **Assigned Service Number** (Zugewiesene Servicenummer) wird eine Problemticketnummer angezeigt.

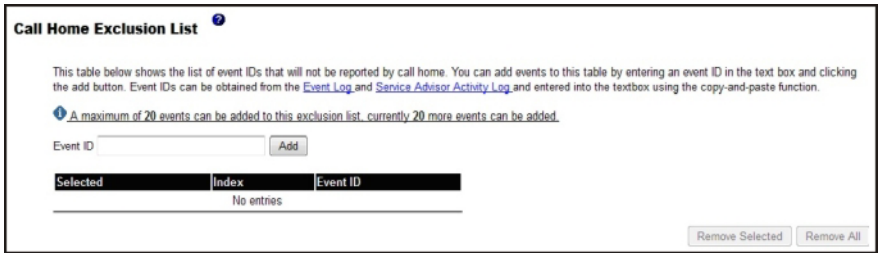
  Pending (Anstehend)
  Das Call-Home-Ereignis ist in Bearbeitung.

  Failed (Fehlgeschlagen)
  Das Call-Home-Ereignis ist fehlgeschlagen. Wenn das Call-Home-Ereignis fehlschlägt, wenden Sie sich an IBM Support, um das Hardware-Service-Ereignis zu melden. Fehlgeschlagene Call-Home-Ereignisse werden nicht erneut versucht.

7. Nachdem Sie ein Ereignis gelöscht haben, klicken Sie auf das Kontrollkästchen **Corrected** (Korrigiert) für das Ereignis, um die Suche nach nicht gelösten Ereignissen einfacher zu machen.

   Anmerkung: Wenn das Kontrollkästchen **Corrected** für ein Ereignis nicht ausgewählt ist, wird ein Auftreten desselben Ereignisses erst wieder fünf Tage nach dem ersten Auftreten des Ereignisses mit der *Call-Home-Funktion gesendet*.
8. Klicken Sie dann auf **Refresh** (Aktualisieren), um die aktuellsten Informationen anzuzeigen.

   Anmerkung: Die Nummer unter **Assigned Service Number** kann als Referenz für das Call-Home-Ereignis verwendet werden, wenn eine Datenübertragung zu IBM Support erfolgt.
9. Gehen Sie wie folgt vor, um ein angegebenes Ereignis aus dem Bericht an IBM Support zu entfernen:
   a. Klicken Sie auf den Link **Call Home Exclusion List** (Call-Home-Ausschlussliste). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



b. Geben Sie im Feld **Event ID** (Ereignis-ID) die hexadezimale Ereignis-ID ein.
c. Klicken Sie auf **Add** (Hinzufügen).

Abmeldung

Klicken Sie im Navigationsfenster auf **Log Off** (Abmelden), um sich vom IMM oder einem anderen fernen Server abzumelden.

Kapitel 4. Serverstatus überwachen

Verwenden Sie die Links unter der Kopfzeile **Monitors** (Überwachungstools) im Navigationsfenster, um den Status des Servers, auf den Sie zugreifen, anzuzeigen.

Auf den Systemstatusseiten können Sie folgende Tasks ausführen:

- Stromversorgungsstatus des Servers überwachen und den Status des Betriebssystems anzeigen
- Temperaturwerte, Spannungsgrenzwerte und Lüftergeschwindigkeiten des Servers anzeigen
- Aktuelle Anzeigenerfassung bei einem Systemabsturz des Servers anzeigen
- Liste der Benutzer anzeigen, die am IMM angemeldet sind

Auf der Seite "Virtual Light Path" können Sie den Namen, die Farbe und den Status sämtlicher Anzeigen anzeigen, die im Server leuchten.

Auf den Ereignisprotokollseite können Sie folgende Tasks ausführen:

- Bestimmte Ereignisse anzeigen, die im Ereignisprotokoll des IMM aufgezeichnet werden
- Schweregrad von Ereignissen anzeigen

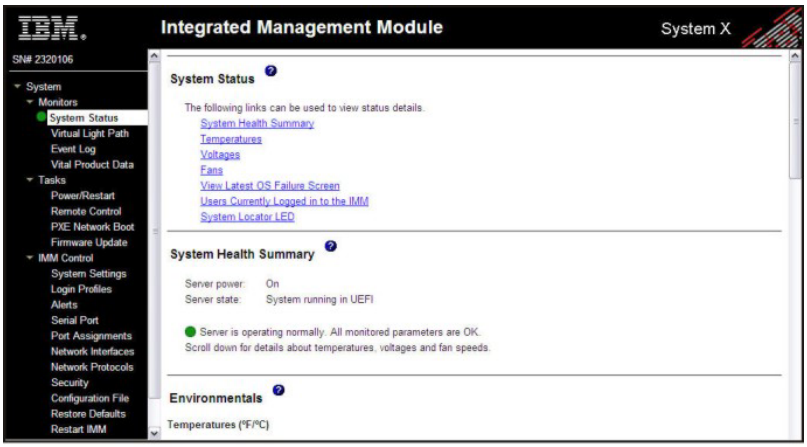
Auf der Seite mit den elementaren Produktdaten (VPD) können Sie diese Daten anzeigen.

Systemstatus anzeigen

Auf der Seite "System Status" können Sie die gemessenen Temperaturwerte, die Spannungsschwellenwerte und den Lüfterstatus Ihres Servers überprüfen. Sie können sich außerdem die neueste Betriebssystemfehleranzeige, die derzeit am IMM angemeldeten Benutzer sowie die Systempositionsanzeige anzeigen lassen.

Gehen Sie wie folgt vor, um sich die Informationen zu Systemzustand und Umgebung des Servers anzeigen zu lassen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **System Status**, um sich eine dynamisch generierte Aktualisierung des allgemeinen Serverzustands anzeigen zu lassen. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



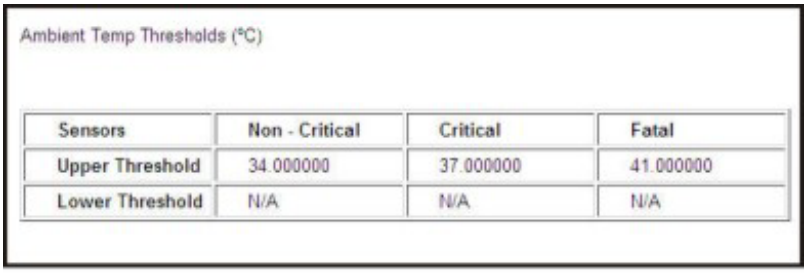
Der Status Ihres Servers bestimmt, welche Nachricht oben auf der Seite "System Health Summary" (Systemzustandsübersicht) angezeigt wird. Eines der folgenden Symbole wird angezeigt:

- Ein ausgefüllter grüner Kreis und die Wortfolge `Server is operating normally` (Server läuft normal)
- Entweder ein roter Kreis mit einem X darin oder ein gelbes Dreieck mit einem Ausrufezeichen sowie der Wortfolge `One or more monitored parameters are abnormal` (Einer oder mehrere der überwachten Parameter ist nicht normal)

Wenn die überprüften Parameter außerhalb des Normalbereichs liegen, wird eine genaue Liste der abnormalen Parameter auf der Seite "System Health Summary" angezeigt.

3. Blättern Sie abwärts zum Bereich **Temperature** im Abschnitt **Environmentals** (Umgebungsfaktoren) der Seite, der Informationen zu Temperatur, Spannung und Lüftergeschwindigkeit enthält.

   Das IMM verfolgt die aktuellen gemessenen Temperaturwerte und Schwellenwerte für Systemkomponenten wie die Mikroprozessoren, die Systemplatine und die Rückwandplatine für Festplattenlaufwerke. Wenn Sie auf einen gemessenen Temperaturwert klicken, wird ein neues Fenster geöffnet.



Auf der Seite "Temperature Thresholds" werden die Temperaturen angezeigt, bei denen das IMM reagiert. Die Temperaturschwellenwerte sind auf dem fernen Server voreingestellt und können nicht geändert werden.

Die dokumentierten Temperaturen werden mit den folgenden Schwellenbereichen abgeglichen:

Non-Critical (Unkritisch)

Wenn die Temperatur einen bestimmten Wert erreicht, wird ein Temperaturalert an die konfigurierten Empfänger der fernen Alerts gesendet. Sie müssen das Kontrollkästchen **Warning Alerts** (Warnungsalerts) im Bereich **SNMP Alerts Settings** (SNMP-Alerteinstellungen) der Seite "Alerts" oder das Kontrollkästchen **Warning Alerts** auf der Seite "Remote Alert Recipient" (Empfänger der fernen Alerts) auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren" auf Seite 37 oder im Abschnitt „Empfänger für ferne Alerts konfigurieren" auf Seite 35.

Critical

Wenn die Temperatur einen bestimmten Wert erreicht, der höher liegt als der Warnwert (den Schwellenwert für einen normalen Systemabschluss), wird ein zweiter Temperaturalert an die konfigurierten Empfänger der fernen Alerts gesendet und der Server beginnt den Systemabschluss mit einem ordnungsgemäßen Betriebssystemabschluss. Der Server schaltet sich daraufhin aus. Sie müssen das Kontrollkästchen **Critical Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" oder das Kontrollkästchen **Critical Alerts** auf der Seite "Remote Alert Recipient" auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren" auf Seite 37 oder im Abschnitt „Empfänger für ferne Alerts konfigurieren" auf Seite 35.

Fatal (Schwerwiegend)

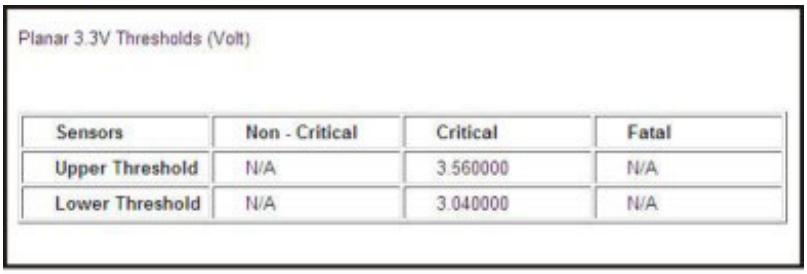
Wenn die Temperatur einen bestimmten Wert erreicht, der höher liegt als der Wert für einen normalen Systemabschluss (den Schwellenwert für einen erzwungenen Systemabschluss), so fährt der Server sofort herunter und sendet einen Alert an die konfigurierten Empfänger der fernen Alerts. Sie müssen das Kontrollkästchen **Critical Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" oder das Kontrollkästchen **Critical Alerts** auf der Seite "Remote Alert Recipient" auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren" auf Seite 37 oder im Abschnitt „Empfänger für ferne Alerts konfigurieren" auf Seite 35.

Das IMM erstellt ein unkritisches oder ein kritisches Ereignis, wenn der Schwellenwert erreicht wird, und leitet bei Bedarf Aktionen zum Systemabschluss ein.

4. Blättern Sie abwärts in den Bereich **Voltages** (Spannungen). Das IMM sendet jedesmal einen Alert, wenn die Spannung einer überwachten Stromquelle außerhalb ihrer angegebenen Betriebsbereiche liegt.

   Wenn Sie auf einen gemessenen Spannungswert klicken, wird ein neues Fenster geöffnet.



Auf der Seite "Voltage Thresholds" (Spannungsschwellenwerte) werden die Spannungsbereiche angezeigt, bei denen das IMM reagiert. Die Spannungsschwellenwerte sind auf dem fernen Server voreingestellt und können nicht geändert werden.

Auf der IMM-Webschnittstelle werden die gemessenen Spannungswerte der Systemplatine und der Spannungsreglermodule (VRM, voltage regulator modules) angezeigt. Das System legt einen Spannungsbereich fest, bei dem die folgenden Aktionen durchgeführt werden:

Non-Critical

Wenn die Spannung einen bestimmten Spannungsbereich unter- oder überschreitet, wird ein Spannungsalert an die konfigurierten Empfänger der fernen Alerts gesendet. Sie müssen das Kontrollkästchen **Warning Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren” auf Seite 37.

Critical

Wenn die Spannung einen bestimmten Spannungsbereich unter- oder überschreitet, wird ein Spannungsalert an die konfigurierten Empfänger der fernen Alerts gesendet und der Server beginnt den Systemabschluss mit einem ordnungsgemäßen Betriebssystemabschluss. Der Server schaltet sich daraufhin aus. Sie müssen das Kontrollkästchen **Critical Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren” auf Seite 37.

Fatal Wenn die Spannung einen bestimmten Spannungsbereich unter- oder überschreitet, fährt der Server sofort herunter und sendet einen Alert an die konfigurierten Empfänger der fernen Alerts. Sie müssen das Kontrollkästchen **Critical Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" auswählen, damit der Alert gesendet wird.

Anmerkung: Der Alert über einen erzwungenen Systemabschluss wird nur gesendet, wenn noch kein Alert über einen normalen Systemabschluss gesendet wurde.

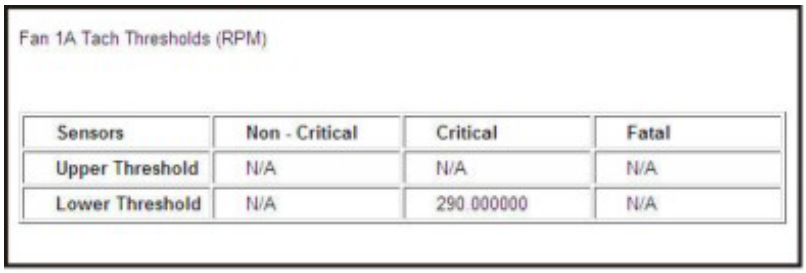
Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren” auf Seite 37.

Das IMM erstellt ein unkritisches oder ein kritisches Ereignis, wenn der Schwellenwert erreicht wird, und leitet bei Bedarf Aktionen zum Systemabschluss ein.

Non-critical
Wenn das IMM angibt, dass dieser Schwellenwert erreicht wurde, wird ein Warnungsereignis erstellt.

Critical
Wenn das IMM angibt, dass dieser Schwellenwert erreicht wurde, wird ein kritisches Ereignis erstellt.

5. Blättern Sie abwärts zum Bereich **Fan Speeds (% of max)** (Lüftergeschwindigkeiten (% der Höchstgeschwindigkeit)). Auf der IMM-Webschnittstelle wird die aktuelle Drehzahl der Serverlüfter (als Prozentsatz der Lüfterhöchstgeschwindigkeit) angezeigt. Wenn Sie auf einen gemessenen Lüfterwert klicken, wird ein neues Fenster geöffnet.



Sie erhalten einen Lüfteralert, wenn die Lüftergeschwindigkeiten auf eine nicht akzeptable Stufe fallen oder wenn die Lüfter anhalten. Sie müssen das Kontrollkästchen **Critical Alerts** im Bereich **SNMP Alerts Settings** der Seite "Alerts" auswählen, damit der Alert gesendet wird.

Weitere Informationen zur Auswahl von Alertoptionen finden Sie im Abschnitt „Einstellungen für SNMP-Alerts konfigurieren" auf Seite 37.

6. Blättern Sie abwärts in den Bereich **View Latest OS Failure Screen** (Letzte Betriebssystem-Fehleranzeige anzeigen). Klicken Sie auf **View OS Failure Screen** (Betriebssystem-Fehleranzeige anzeigen), um auf ein Bild von der Betriebssystemfehleranzeige zugreifen zu können, das aufgezeichnet wurde, als der Server seine Funktionen einstellte.

Anmerkung:

Die Funktion zur Aufzeichnung der Betriebssystemfehleranzeige ist nur mit IMM Premium verfügbar. Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade von IMM Standard auf IMM Premium durchführen" auf Seite 6.

Bei einem Ereignis, das zum Ausschalten des Betriebssystems führt, wird der Betriebssystem-Watchdog ausgelöst, woraufhin das IMM die Daten der Betriebssystemfehleranzeige aufzeichnet und speichert. Das IMM speichert nur die Informationen zu den aktuellsten Fehlerereignissen und überschreibt die Daten älterer Betriebssystemfehleranzeigen, wenn ein neues Fehlerereignis auftritt.

Gehen Sie wie folgt vor, um über Fernzugriff auf das Bild von der Betriebssystemfehleranzeige eines Servers zuzugreifen:

a. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
b. Klicken Sie im Navigationsfenster auf **System Health** (Systemzustand) und blättern Sie abwärts zum Bereich **View Latest OS Failure Screen**.
c. Klicken Sie auf **View OS Failure Screen**. Das Bild von der Betriebssystemfehleranzeige wird auf Ihrem Bildschirm angezeigt.

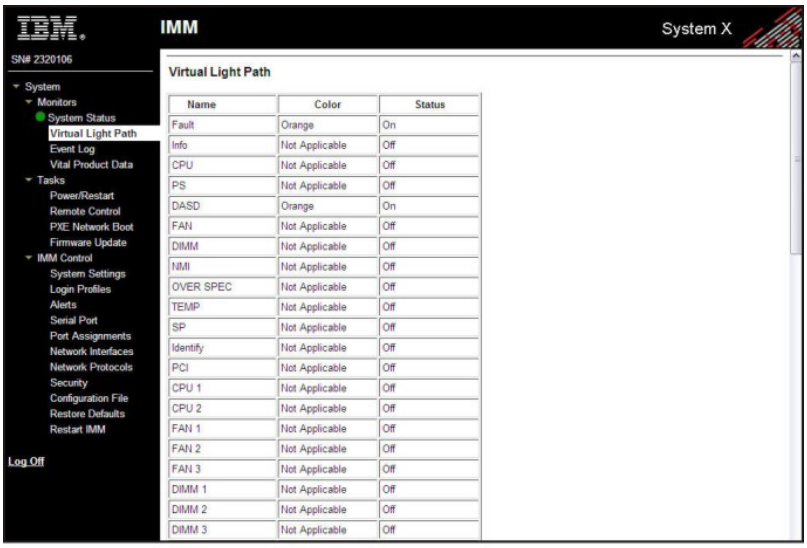
7. Blättern Sie abwärts in den Bereich **Users Currently Logged in** (Derzeit angemeldete Benutzer). Auf der IMM-Webschnittstelle werden Anmelde-ID und Zugriffsmethode jedes Benutzers angezeigt, der am IMM angemeldet ist.
8. Blättern Sie abwärts in den Bereich **System Locator LED** (Systempositionsanzeige). Auf der IMM-Webschnittstelle wird der Status der Systempositionsanzeige angezeigt. Sie verfügt auch über Schaltflächen zum Ändern des Anzeigenzustands. Informationen zur Bedeutung der Grafiken, die in diesem Bereich angezeigt werden, finden Sie in der Onlinehilfe.

"Virtual Light Path" anzeigen

Auf der Anzeige des "Virtual Light Path" sind Name, Farbe und Status sämtlicher Anzeigen angegeben, die im Server leuchten.

Gehen Sie wie folgt vor, um auf den "Virtual Light Path" zuzugreifen und ihn anzeigen zu lassen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Virtual Light Path**, um sich den aktuellen Ereignisverlauf des Servers anzeigen zu lassen. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Blättern Sie abwärts, um sich den vollständigen Inhalt des "Virtual Light Path" anzeigen zu lassen.

   Anmerkung: Wenn eine Anzeige im Server nicht leuchtet, zeigt die Spalte "Color" (Farbe) der "Virtual Light Path"-Tabelle an, dass die Anzeige Color "Not Applicable" (Nicht anwendbar) ist.

Ereignisprotokolle anzeigen

Anmerkung: Erklärungen zu den einzelnen Ereignissen und Nachrichten finden Sie in der Dokumentation zu Ihrem Server.
Fehlercodes und -nachrichten werden in den folgenden Ereignisprotokolltypen angezeigt:

- **System-event log** (Systemereignisprotokoll): Dieses Protokoll enthält POST- und SMI-Ereignisse (SMI - System Management Interrupt) sowie alle Ereignisse, die von dem in IMM integrierten BMC generiert wurden. Sie können das Systemereignisprotokoll mithilfe des Konfigurationsdienstprogramms und des DSA-Programms (DSA - Dynamic System Analysis) (als IPMI-Ereignisprotokoll) anzeigen.

  Das Systemereignisprotokoll hat eine begrenzte Größe. Wenn es voll ist, werden die vorhandenen Einträge nicht von neuen Einträgen überschrieben. Die Einträge im Systemereignisprotokoll müssen daher mithilfe des Konfigurationsdienstprogramms regelmäßig gespeichert und anschließend aus dem Protokoll gelöscht werden. Bei der Fehlerbehebung müssen die Einträge möglicherweise gespeichert und anschließend aus dem Systemereignisprotokoll gelöscht werden, damit die neuesten Ereignisse für die Analyse verfügbar sind.

  Nachrichten werden auf der linken Seite des Bildschirms und Details zur ausgewählten Nachricht auf der rechten Seite des Bildschirms angezeigt. Verwenden Sie die Tasten mit dem Aufwärtspfeil (↑) und dem Abwärtspfeil (↓), um von einem Eintrag zum nächsten zu gelangen.

  Das Systemereignisprotokoll gibt ein Assertion-Ereignis an, wenn ein Ereignis aufgetreten ist. Es gibt ein Deassertion-Ereignis an, wenn das Ereignis nicht mehr auftritt.

  Einige IMM-Sensoren führen dazu, dass Assertion-Ereignisse protokolliert werden, wenn ihre Sollwerte erreicht sind. Wenn eine Sollwertbedingung nicht mehr vorhanden ist, wird ein entsprechendes Deassertion-Ereignis protokolliert. Jedoch zählen nicht alle Ereignisse zum Typ "Assertion-Ereignis".
- **Integrated management module (IMM) event log** (Ereignisprotokoll des integrierten Managementmoduls (IMM)): Dieses Protokoll enthält eine gefilterte Teilmenge aller IMM-, POST- und SMI- Ereignisse. Sie können das IMM-Ereignisprotokoll mithilfe der IMM-Webschnittstelle und des DSA-Programms (als ASM-Ereignisprotokoll) anzeigen.
- **DSA log** (DSA-Protokoll): Dieses Protokoll wird vom Programm "Dynamic System Analysis" (DSA) generiert und ist eine chronologisch geordnete Zusammenführung des Systemereignisprotokolls (als IPMI-Ereignisprotokoll), des IMM-Gehäuseereignisprotokolls (als ASM-Ereignisprotokoll) und der Ereignisprotokolle des Betriebssystems. Sie können das DSA-Protokoll mithilfe des DSA-Programms anzeigen.
- **Chassis-event log** (Gehäuseereignisprotokoll): Das IMM generiert Textnachrichten für die IPMI-Assertion- und -Deassertion-Ereignisse und erstellt Einträge für sie im Gehäuseereignisprotokoll. Der Text für diese Ereignisse wird durch die DMTF-Spezifikationen (Distributed Management Task Force) DSP0244 und DSP8007 generiert. Dieses Protokoll enthält außerdem Einträge für andere Ereignisse als IPMI-Sensor-Assertion- und -Deassertion-Ereignisse. Das Gehäuseereignisprotokoll enthält z. B. auch Einträge, wenn ein Benutzer eine Netzeinstellung ändert oder wenn ein Benutzer sich an der Webschnittstelle anmeldet. Dieses Protokoll kann über die IMM-Webschnittstelle angezeigt werden.

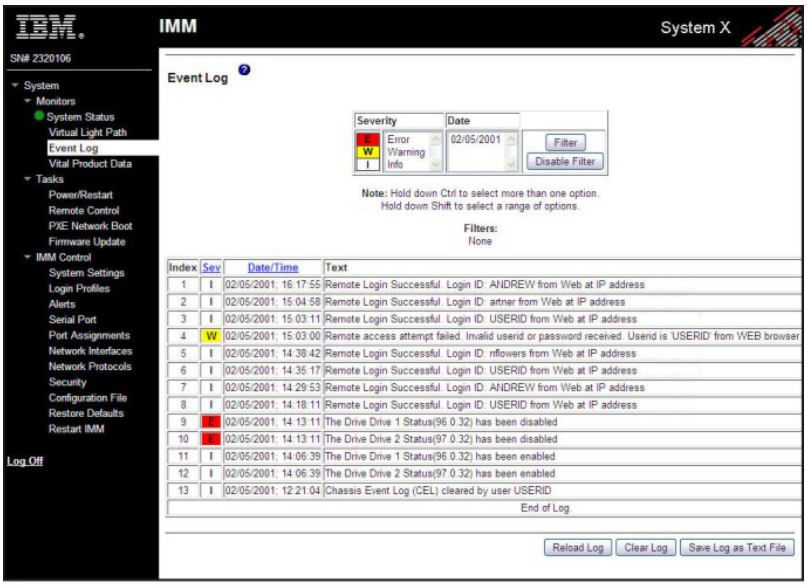
Systemereignisprotokoll aus der Webschnittstelle anzeigen

Anmerkung: Die Kapazität des Systemereignisprotokolls ist begrenzt. Bei Erreichen der Grenze werden immer die ältesten Ereignisse zuerst gelöscht.

Gehen Sie wie folgt vor, um auf das Ereignisprotokoll zuzugreifen und es anzuzeigen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.

2. Klicken Sie im Navigationsfenster auf **Event Log** (Ereignisprotokoll), um sich den aktuellen Ereignisverlauf des Servers anzeigen zu lassen. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Blättern Sie abwärts, um sich den vollständigen Inhalt des Ereignisprotokolls anzeigen zu lassen. Die Ereignisse werden folgenden Bewertungsstufen zugeordnet:

   Information
   Diese Bewertungsstufe wird einem Ereignis zugeordnet, das Sie zur Kenntnis nehmen sollten.

   Warnung
   Diese Bewertungsstufe wird einem Ereignis zugeordnet, das sich möglicherweise auf die Serverleistung auswirken kann.

   Fehler Diese Bewertungsstufe wird einem Ereignis zugeordnet, das sofortige Aufmerksamkeit erfordert.

   Die IMM-Webschnittstelle unterscheidet zwischen Warnungsereignissen mit dem Buchstaben "W" auf gelbem Hintergrund in der Schweregradsäule und Fehlerereignissen mit dem Buchstaben "E" auf rotem Hintergrund.

4. Klicken Sie auf **Save Log as Text File**, um den Inhalt des Ereignisprotokolls als Textdatei zu speichern. Klicken Sie auf **Reload Log** (Protokoll erneut laden), um die Anzeige des Ereignisprotokolls zu aktualisieren. Klicken Sie auf **Clear Log** (Protokollinhalt löschen), um den Inhalt des Ereignisprotokolls zu löschen.

Ereignisprotokolle aus dem Konfigurationsdienstprogramm anzeigen

Ausführliche Informationen zur Verwendung des Konfigurationsdienstprogramms finden Sie in der Dokumentation, die mit Ihrem Server geliefert wurde.

Gehen Sie wie folgt vor, um das POST-Ereignisprotokoll oder das Systemereignisprotokoll anzuzeigen:

1. Schalten Sie den Server ein.

   Anmerkung: Der Netzschalter wird etwa 2 Minuten nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.

2. Wenn die Aufforderung <F1> Setup (F1 für Konfiguration) angezeigt wird, drücken Sie die Taste F1. Wenn Sie ein Startkennwort und ein Administratorkennwort festgelegt haben, müssen Sie das Administratorkennwort eingeben, um die Ereignisprotokolle anzuzeigen.
3. Wählen Sie **Systemereignisprotokolle** aus und verwenden Sie eine der folgenden Vorgehensweisen:
   - Wählen Sie **POST-Ereignisanzeige** aus, um das POST-Ereignisprotokoll anzuzeigen.
   - Wählen Sie **Systemereignisprotokoll** aus, um das Systemereignisprotokoll anzuzeigen.

Ereignisprotokolle ohne Neustart des Servers anzeigen

Wenn der Server nicht blockiert ist, stehen Ihnen Methoden zur Verfügung, um mindestens ein Ereignisprotokoll anzuzeigen, ohne den Server erneut starten zu müssen.

Wenn Sie Portable Dynamic System Analysis (DSA) oder Installable Dynamic System Analysis installiert haben, können Sie damit das Systemereignisprotokoll (als IPMI-Ereignisprotokoll), das IMM-Ereignisprotokoll (als ASM-Ereignisprotokoll), die Ereignisprotokolle des Betriebssystems oder das zusammengefasste DSA-Protokoll anzeigen. Zur Anzeige dieser Protokolle können Sie auch DSA Preboot verwenden. Allerdings müssen Sie zur Verwendung von DSA Preboot den Server erneut starten. Informationen zur Installation von Portable DSA, Installable DSA oder DSA Preboot oder zum Herunterladen eines DSA Preboot-CD-Image finden Sie unter http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000008 oder gehen Sie wie folgt vor.

Anmerkung: Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die tatsächliche Vorgehensweise weicht möglicherweise geringfügig von der Beschreibung im vorliegenden Dokument ab.

1. Öffnen Sie http://www.ibm.com/systems/support/.
2. Klicken Sie unter **Product support** (Produktunterstützung) auf **System x**.
3. Klicken Sie unter **Popular links** (Häufig genutzte Links) auf **Software and device drivers** (Software und Einheitentreiber).
4. Klicken Sie unter **Related downloads** (Zugehörige Downloads) auf **Dynamic System Analysis (DSA)**, um die Matrix mit den herunterladbaren DSA-Dateien anzuzeigen.

Wenn IPMItool auf dem Server installiert ist, können Sie das Programm verwenden, um das Systemereignisprotokoll anzuzeigen. Die neuesten Versionen des Linux-Betriebssystems werden mit der aktuellen IPMItool-Version geliefert. Wenn Sie Informationen zu IPMItool suchen, rufen Sie die Website http://sourceforge.net/ auf.

Anmerkung: Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die tatsächliche Vorgehensweise weicht möglicherweise geringfügig von der Beschreibung im vorliegenden Dokument ab.

1. Öffnen Sie http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp.
2. Klicken Sie im Navigationsfenster auf **IBM System x and BladeCenter Tools Center**.
3. Erweitern Sie nacheinander **Tools reference** (Verweis auf Tools), **Configuration tools** und **IPMI tools** und klicken Sie dann auf **IPMItool**.

Einen Überblick über IPMI bekommen Sie unter http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm oder gehen Sie wie folgt vor:

1. Öffnen Sie http://publib.boulder.ibm.com/infocenter/systems/index.jsp.
2. Klicken Sie im Navigationsfenster auf **IBM Systems Information Center**.
3. Erweitern Sie nacheinander **Operating systems** (Betriebssysteme), **Linux information** und **Blueprints for Linux on IBM systems** (Entwürfe für Linux auf IBM-Systemen) und klicken Sie dann auf **Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms** (IPMI (Intelligent Platform Management Interface) auf IBM Linux-Plattformen verwenden).

Sie können das IMM-Ereignisprotokoll mithilfe des Links **Event Log** (Ereignisprotokoll) in der Webschnittstelle von IMM anzeigen.

In der folgenden Tabelle sind die Methoden beschrieben, die Sie je nach Zustand des Servers zum Anzeigen der Ereignisprotokolle verwenden können. Bei den ersten beiden Zuständen ist ein Neustart des Servers nicht erforderlich.

Tabelle 16. Methoden zum Anzeigen von Ereignisprotokollen

Zustand	Maßnahme
Der Server ist nicht blockiert und ist mit einem Netz verbunden.	Verwenden Sie eine der folgenden Methoden: • Führen Sie Portable oder Installable DSA aus, um die Ereignisprotokolle anzuzeigen oder erstellen Sie eine Ausgabedatei, die Sie an die IBM Service- und Unterstützungsfunktion senden können. • Geben Sie die IP-Adresse des IMM ein und rufen Sie die Seite "Event Log" auf. • Verwenden Sie IPMItool, um das Systemereignisprotokoll anzuzeigen.
Der Server ist nicht blockiert und nicht mit einem Netz verbunden.	Verwenden Sie IPMItool lokal, um das Systemereignisprotokoll anzuzeigen.
Der Server ist blockiert.	• Wenn DSA Preboot installiert ist, starten Sie den Server erneut und drücken Sie die Taste F2, um DSA Preboot zu starten und die Ereignisprotokolle anzuzeigen. • Wenn DSA Preboot nicht installiert ist, legen Sie die DSA Preboot-CD ein und starten Sie den Server erneut, um DSA Preboot zu starten und die Ereignisprotokolle anzuzeigen. • Sie können den Server auch erneut starten und die Taste F1 drücken, um das Konfigurationsdienstprogramm zu starten und das POST-Ereignisprotokoll oder das Systemereignisprotokoll anzuzeigen. Weitere Informationen finden Sie im Abschnitt „Ereignisprotokolle aus dem Konfigurationsdienstprogramm anzeigen” auf Seite 118.

Elementare Produktdaten anzeigen

Wenn der Server gestartet wird, sammelt das IMM Serverinformationen, Server-Firmwareinformationen und elementare Produktdaten (VPD - vital product data) von Serverkomponenten und speichert sie im nicht flüchtigen Speicher. Sie haben jederzeit von nahezu jedem Computer aus Zugriff auf diese Informationen. Die Seite "Vital Product Data" (Elementare Produktdaten) enthält Schlüsselinformationen zum fernverwalteten Server, der vom IMM überwacht wird.

Gehen Sie wie folgt vor, um die elementaren Produktdaten von Serverkomponenten anzeigen zu lassen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Vital Product Data**, um den Status der Hardware- und Softwarekomponenten des Servers anzeigen zu lassen.
3. Blättern Sie abwärts, um die folgenden gemessenen Werte der elementaren Produktdaten anzuzeigen:

   Machine level VPD (Elementare Produktdaten auf Maschinenebene)
   Die elementaren Produktdaten des Servers erscheinen in diesem Bereich. Zum Anzeigen der elementaren Produktdaten schließen die elementaren Produktdaten auf Maschinenebene einen Universal Unique Identifier (UUID) mit ein.

   Anmerkung: Die elementaren Produktdaten auf Maschinenebene und Komponentenebene sowie das Komponentenaktivitätenprotokoll geben nur dann Informationen an, wenn der Server eingeschaltet ist.

Tabelle 17. Elementare Produktdaten auf Maschinenebene

Feld	Funktion
Machine type and model	Bestimmt Typ und Modellnummer des Servers, der vom IMM überwacht wird.
Serial number	Bestimmt die Seriennummer des Servers, der vom IMM überwacht wird.
UUID	Bestimmt den Universal Unique Identifier (UUID) - eine 32-stellige Hexadezimalzahl - des Servers, der vom IMM überwacht wird.

Component Level VPD (Elementare Produktdaten auf Komponentenebene)
Die elementaren Produktdaten der Komponenten des fernverwalteten Servers werden in diesem Bereich angezeigt.

Tabelle 18. Elementare Produktdaten auf Komponentenebene

Feld	Funktion
FRU name	Bestimmt die FRUs (Field Replaceable Units, durch den Kundendienst austauschbare Funktionseinheiten) für jede Komponente.
Serial number	Bestimmt die Seriennummer jeder Komponente.
Mfg ID	Bestimmt die Hersteller-ID jeder Komponente.

Component Activity Log (Komponentenaktivitätenprotokoll)
Sie können sich einen Bericht der Komponentenaktivität in diesem Bereich anzeigen lassen.

Tabelle 19. Komponentenaktivitätenprotokoll

Feld	Funktion
FRU name	Bestimmt den FRU-Namen (Field Replaceable Unit, durch den Kundendienst austauschbare Funktionseinheit) der Komponente.
Serial number	Bestimmt die Seriennummer der Komponente.
Mfg ID	Bestimmt den Hersteller der Komponente.
Action (Maßnahme)	Bestimmt die erforderliche Maßnahme für jede Komponente.
Timestamp (Zeitmarke)	Bestimmt Datum und Uhrzeit der Komponentenmaßnahme. Das Datum wird im Format *MM/TT/JJ* angezeigt. Die Uhrzeit wird im Format *hh:mm:ss* angezeigt.

IMM VPD (Elementare Produktdaten des IMM)

Sie können sich die elementaren Produktdaten der IMM-Firmware, der Server-Firmware für System x und der Dynamic System Analysis-Firmware des fernverwalteten Servers in diesem Bereich anzeigen lassen.

Tabelle 20. Elementare Produktdaten für IMM-, UEFI- und DSA-Firmware

Feld	Funktion
Firmware type	Gibt den Firmware-Codetyp an.
Version string (Versionszeichenfolge)	Gibt die Firmware-Codeversion an.
Release date	Gibt an, wann die Firmware freigegeben wurde.

Kapitel 5. IMM-Tasks ausführen

Verwenden Sie die folgenden Funktionen unter der Kopfzeile **Tasks** im Navigationsfenster, um die Aktionen des IMM und Ihres Servers direkt zu steuern. Die Tasks, die Sie ausführen können, richten sich nach dem Server, in dem das IMM installiert ist.

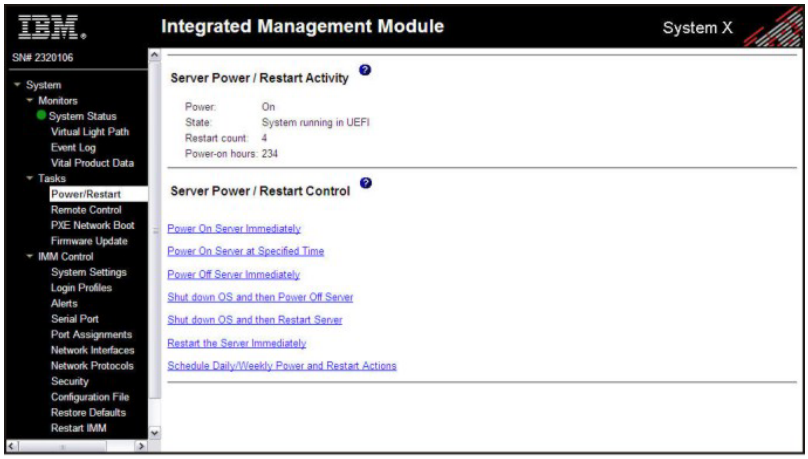
Sie können die folgenden Tasks ausführen:

- Serverstromversorgung und Neustartaktivitäten anzeigen
- Stromversorgungsstatus des Servers über Fernzugriff steuern
- Serverkonsole über Fernzugriff verwenden
- Eine Platte oder ein Plattenimage über Fernzugriff an den Server anhängen
- IMM-Firmware aktualisieren

Anmerkung: Einige Produktmerkmale sind nur auf Servern verfügbar, auf denen ein unterstütztes Microsoft Windows-Betriebssystem ausgeführt wird.

Serverstromversorgung und Neustartaktivitäten anzeigen

Im Bereich **Server Power/Restart Activity** (Serverstromversorgung/ Neustartaktivität) wird der Stromversorgungsstatus des Servers zum Zeitpunkt der Generierung der Webseite angezeigt.



Power (Stromversorgung)
In diesem Feld wird der Stromversorgungsstatus des Servers zum Zeitpunkt der Generierung der aktuellen Webseite angezeigt.

Status In diesem Feld wird der Zustand des Servers zum Zeitpunkt der Generierung der aktuellen Webseite angezeigt. Die folgenden Zustände sind möglich:

- System power off/State unknown (Stromversorgung des Systems ausgeschaltet/Status unbekannt)
- System on/starting UEFI (System eingeschaltet/UEFI wird gestartet)
- System stopped in UEFI (Error detected) (System in UEFI gestoppt - Fehler festgestellt)
- System running in UEFI (System wird in UEFI ausgeführt)

- Booting OS or in unsupported OS (Betriebssystem wird gebootet oder nicht unterstütztes Betriebssystem) (dies kann eintreten, wenn das Betriebssystem nicht für die Unterstützung der Inbandschnittstelle für das IMM konfiguriert ist)
- OS booted (Betriebssystem gebootet)

Restart count (Zähler für Neustart)
In diesem Feld wird die Anzahl der Serverneustarts angezeigt.

Anmerkung: Der Zähler wird auf null zurückgesetzt, wenn das IMM-Subsystem auf die werkseitigen Voreinstellungen zurückgesetzt wird.

Power-on hours (Eingeschaltet - Stunden)
In diesem Feld wird die Gesamtanzahl an Stunden angezeigt, die der Server bereits eingeschaltet ist.

Einschaltstatus eines Servers steuern

Das IMM stellt eine vollständige Einschaltsteuerung Ihres Servers bereit, einschließlich Aktionen zu Einschalten, Ausschalten und erneut Starten. Außerdem werden die Statistikdaten zum Einschalten und Neustart erfasst und angezeigt, um die Verfügbarkeit der Server-Hardware anzugeben. Um die Aktionen im Bereich **Server Power/Restart Control** (Steuerung von Einschalten/Neustart des Servers) ausführen zu können, müssen Sie über Supervisorzugriff auf das IMM verfügen.

Gehen Sie wie folgt vor, um Aktionen zum Einschalten und zum Neustart des Servers auszuführen.

Anmerkung: Wählen Sie die folgenden Optionen nur im Notfall aus oder wenn Sie sich an einem anderen Standort befinden und der Server nicht mehr reagiert.

1. Melden Sie sich am IMM an. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Power/Restart** (Einschalten/Neustart). Blättern Sie abwärts bis zum Bereich **Server Power/Restart Control**.
3. Klicken Sie auf eine der folgenden Optionen:

Power on server immediately (Server sofort einschalten)
Server einschalten und das Betriebssystem starten.

Power on server at specified time (Server zu einer bestimmten Zeit einschalten)
Server zu einer bestimmten Zeit einschalten und das Betriebssystem starten.

Power off server immediately (Server sofort ausschalten)
Server ausschalten, ohne das Betriebssystem herunterzufahren.

Shut down OS and then power off server (Betriebssystem herunterfahren und Server ausschalten)
Betriebssystem herunterfahren und den Server anschließend ausschalten.

Anmerkung: Falls sich das Betriebssystem im Bildschirmschonermodus oder im gesperrten Modus befindet, wenn die Anforderung "Shut down OS and then power off server" gesendet wird, kann das IMM möglicherweise keinen ordnungsgemäßen Systemabschluss einleiten. Das IMM führt dann einen Kaltstart oder einen Systemabschluss nach Ablaufen des Ausschaltverzögerungsintervalls durch, während das Betriebssystem möglicherweise noch ausgeführt wird.

Shut down OS and then restart server (Betriebssystem herunterfahren und Server erneut starten)
Betriebssystem erneut starten.

Anmerkung: Falls sich das Betriebssystem im Bildschirmschonermodus oder im gesperrten Modus befindet, wenn die Anforderung "Shut down OS and then restart server" gesendet wird, kann das IMM möglicherweise keinen ordnungsgemäßen Systemabschluss einleiten. Das IMM führt dann einen Kaltstart oder einen Systemabschluss nach Ablaufen des Ausschaltverzögerungsintervalls durch, während das Betriebssystem möglicherweise noch ausgeführt wird.

Restart the server immediately (Server sofort erneut starten)
Server ausschalten und anschließend sofort wieder einschalten, ohne das Betriebssystem herunterzufahren.

Schedule daily/weekly power and restart actions (Tägliche/Wöchentliche Aktionen zum Einschalten und erneuten Starten planen)
Das Betriebssystem herunterfahren und den Server täglich oder wöchentlich zu einer festgelegten Uhrzeit ausschalten (mit oder ohne Neustart des Servers) und den Server täglich oder wöchentlich zu einer festgelegten Uhrzeit einschalten.

Wenn Sie eine dieser Optionen auswählen, wird eine Bestätigungsnachricht angezeigt und Sie können die Operation abbrechen, falls Sie sie unbeabsichtigt ausgewählt haben.

Remote Presence

Anmerkung:

1. Die Remote Presence-Funktion des IMM ist nur in IMM Premium verfügbar. Weitere Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade von IMM Standard auf IMM Premium durchführen” auf Seite 6.
2. Die Fernsteuerungsfunktion ist nur über die IMM-Webschnittstelle verfügbar. Sie müssen sich am IMM mit einer Benutzer-ID anmelden, die über Supervisorzugriff verfügt, um die Fernsteuerungsfunktionen verwenden zu können.

Sie können die Remote Presence-Funktion oder die Fernsteuerungsfunktion in der IMM-Webschnittstelle zum Anzeigen und Interagieren mit der Serverkonsole verwenden. Sie können dem Server außerdem ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk, ein USB-Flashlaufwerk oder ein Plattenimage zuordnen, das sich auf Ihrem Computer befindet.

Die Fernsteuerungsfunktion stellt die folgenden Funktionen bereit:

- Anzeige mit einer Grafikauflösung bis zu 1280 x 1024 bei 75 Hz über Fernzugriff aufrufen, unabhängig vom Serverzustand
- Fernzugriff auf den Server unter Verwendung der Tastatur und Maus eines fernen Clients
- Zuordnung des CD- oder DVD-Laufwerks, des Diskettenlaufwerks und des USB-Flashlaufwerks auf einem fernen Client; Zuordnung von ISO- und Diskettenimagedateien als virtuelle Laufwerke, die zur Verwendung durch den Server verfügbar sind
- Hochladen eines Diskettenimages in den IMM-Speicher und Zuordnen dieses Images zu einem Server als virtuelles Laufwerk

Ihre IMM-Firmware und Java- oder ActiveX-Applet aktualisieren

Wichtig: Das IMM verwendet ein Java-Applet oder ein ActiveX-Applet, um die Remote-Presence-Funktion auszuführen. Wenn das IMM auf die neueste Firmwareversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den örtlichen Zwischenspeicher. Nach einem Flash-Update der IMM-Firmware ist das vom Server verwendete Java-Applet möglicherweise nicht auf dem neuesten Stand.

Gehen Sie wie folgt vor, um diese Problem zu beheben:

1. Klicken Sie auf **Start → Settings (Einstellungen) → Control Panel (Steuerkonsole)**.
2. Klicken Sie zweimal auf **Java Plug-in 1.5**. Das Fenster "Control Panel" des Java-Plug-in wird geöffnet.
3. Klicken Sie auf die Registerkarte **Cache** (Zwischenspeicher).
4. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie das Kontrollkästchen **Enable Caching** (Zwischenspeichern aktivieren) ab, damit die Java-Zwischenspeicherung immer inaktiviert ist.
   - Klicken Sie auf **Clear Caching** (Zwischenspeichern abwählen). Wenn Sie diese Option wählen, müssen Sie nach jeder IMM-Firmwareaktualisierung auf **Clear Caching** klicken.

Weitere Informationen zur Aktualisierung von IMM-Firmware finden Sie im Abschnitt „Firmware aktualisieren" auf Seite 137.

Remote Presence-Funktion aktivieren

Anmerkung: Die Remote Presence-Funktion des IMM ist nur in IMM Premium verfügbar. Weitere Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade von IMM Standard auf IMM Premium durchführen" auf Seite 6.

Gehen Sie wie folgt vor, um die Remote-Presence-Funktion zu aktivieren:

1. Unterbrechen Sie die Stromversorgung des Servers, indem Sie das Netzkabel vom Server abziehen.
2. Installieren Sie den Virtual Media Key in den hierfür vorgesehenen Steckplatz auf der Systemplatine.
3. Schließen Sie den Server wieder an die Stromversorgung an.

   Anmerkung: Der Netzschalter wird etwa 2 Minuten nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.
4. Schalten Sie den Server ein.

Fernsteuerung

Die Fernsteuerungsfunktion von IMM besteht aus zwei Java-Anwendungen in zwei separaten Fenstern:

Video Viewer

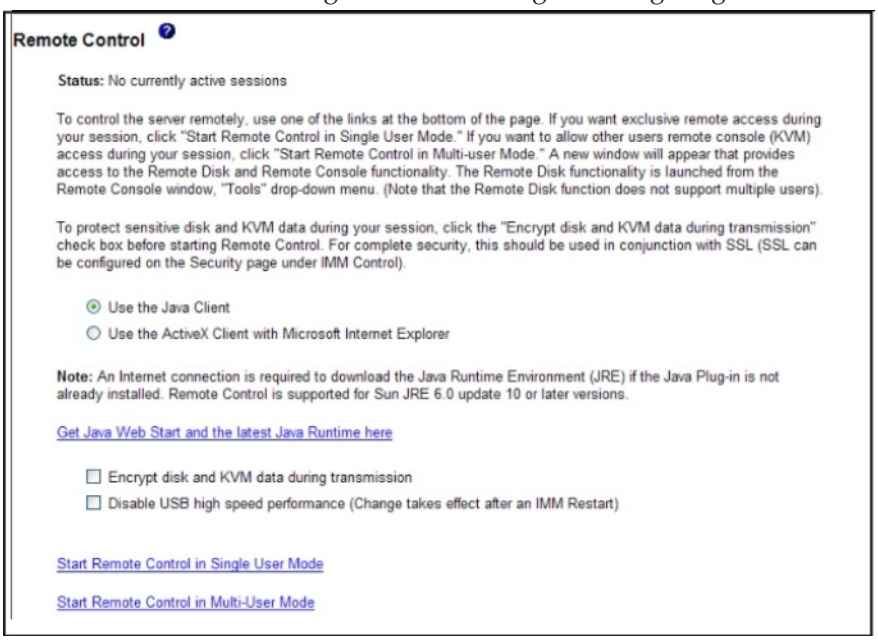
Der Video Viewer verwendet eine ferne Konsole für die Verwaltung ferner Systeme. Bei einer fernen Konsole handelt es sich um eine interaktive Anzeige der grafischen Benutzeroberfläche (GUI) des Servers, die auf Ihrem

Computer angezeigt wird. Sie sehen auf Ihrem Bildschirm genau, was auf der Serverkonsole angezeigt wird, und Sie können die Konsole per Tastatur und Maus steuern.

Virtual Media Session
Im Fenster "Virtual Media Session" sind alle Laufwerke auf dem Client aufgelistet, die den fernen Laufwerken zugeordnet werden können. Dies ermöglicht die Zuordnung von ISO- und Diskettenimage-Dateien als virtuelle Laufwerke. Jedes zugeordnete Laufwerk kann als schreibgeschützt markiert werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt.

Gehen Sie wie folgt vor, um über Fernzugriff auf eine Serverkonsole zuzugreifen:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Remote Control** (Fernsteuerung). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Use the Java Client** (Java-Client verwenden), um mit dem Java-Applet die Remote-Presence-Funktion auszuführen.
   - Klicken Sie zum Verwenden des Internet Explorer in Windows Operating Systems auf **Use the ActiveX Client with Microsoft Internet Explorer** (ActiveX Client mit Microsoft Internet Explorer verwenden) und verwenden Sie das ActiveX-Applet, um die Remote-Presence-Funktion auszuführen.

     Anmerkung: Der 32-Bit Remote-Presence-Client von ActiveX ist mit der IMM-Firmwareversion 1.28 und späteren Versionen verfügbar. Der 64-Bit ActiveX-Client ist mit der IMM-Firmwareversion 1.30 und späteren Versionen verfügbar.
4. Verwenden Sie zum Steuern des Servers über Fernzugriff einen der Links unten auf der Seite "Remote Control". Wenn Sie während Ihrer Sitzung exklusiven Fernzugriff möchten, klicken Sie auf **Start Remote Control in Single User Mode** (Fernsteuerung im Einzelbenutzermodus starten). Wenn Sie möchten, dass während Ihrer Sitzung auch andere Benutzer auf die ferne Konsole (KVM) zugreifen können, klicken Sie auf **Start Remote Control in Multi-user Mode**

(Fernsteuerung im Mehrbenutzermodus starten). Neue Fenster werden geöffnet, die den Zugriff auf die Funktionalitäten des fernen Datenträgers und der fernen Konsole ermöglichen.

Wenn vor dem Öffnen des Fensters "Remote Control" das Kontrollkästchen **Encrypt disk and KVM data during transmission** (Disketten- und KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Datenträgerdaten mit ADES verschlüsselt.

Schließen Sie die Fenster "Video Viewer" und "Virtual Media Session", wenn Sie mit dem Verwenden der Funktion "Remote Control" fertig sind.

Anmerkungen:

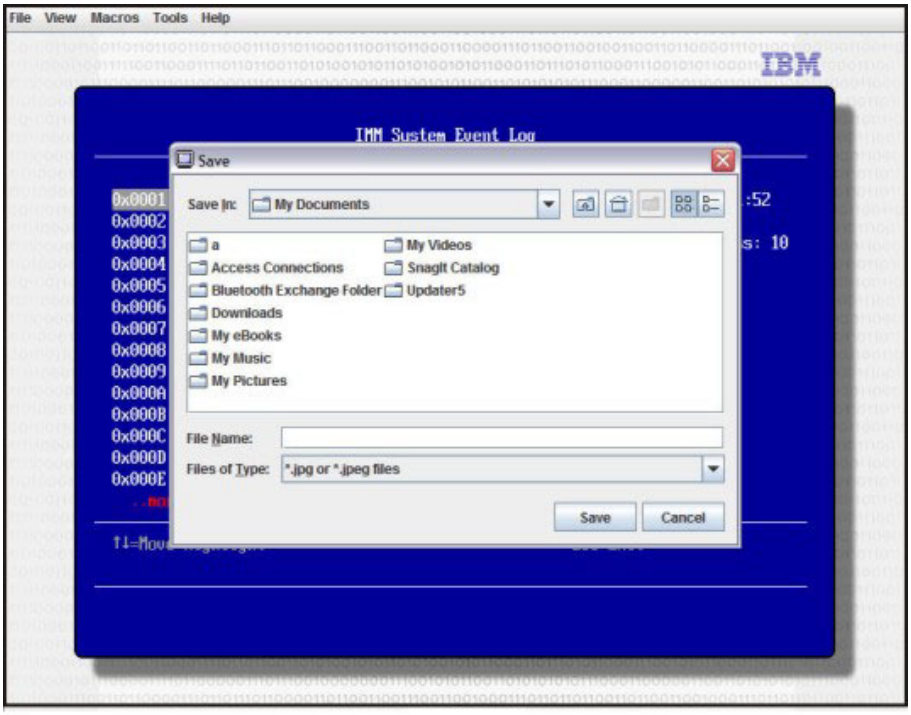
1. Schließen Sie das Fenster "Virtual Media Session" nicht, wenn derzeit ein ferner Datenträger zugeordnet ist. Informationen zum Schließen und zum Trennen der Zuordnung eines fernen Datenträgers finden Sie im Abschnitt„Ferner Datenträger” auf Seite 134.
2. Wenn beim Verwenden der Funktion "Remote Control" Probleme mit der Maus oder der Tastatur auftreten, finden Sie hierzu Hilfe auf der Seite "Remote Control" in der Webschnittstelle.
3. Wenn Sie die ferne Konsole dazu verwenden, im Konfigurationsdienstprogramm Einstellungen des IMM zu ändern, kann es sein, dass der Server das IMM erneut startet. Die Verbindung zur fernen Konsole und die Anmeldesitzung werden abgebrochen. Nach einer kurzen Verzögerung können Sie sich mit einer neuen Sitzung erneut am IMM anmelden, die ferne Konsole erneut starten und das Konfigurationsdienstprogramm verlassen.

Anzeigenerfassung per Fernsteuerung

Die Anzeigenerfassungsfunktion im Fenster Video Viewer erfasst die Inhalte des Serverbildschirms. Gehen Sie wie folgt vor, um eine Bildschirmanzeige zu erfassen und zu speichern:

1. Klicken Sie im Fenster Video Viewer auf **File** (Datei).
2. Wählen Sie aus dem Menü **Capture to File** aus.
3. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für die Bilddatei ein und speichern Sie sie an dem Ort, den Sie auf dem lokalen Client auswählen.

   Anmerkung: Anzeigenerfassungsbilder werden als JPG- oder JPEG- Dateitypen gespeichert.



Ansichtsmodi der Fernsteuerung im Video Viewer

Um die Ansicht im Fenster "Video Viewer" zu ändern, klicken Sie auf **View** (Ansicht). Die folgenden Menüoptionen sind verfügbar:

Refresh (Aktualisieren)
Der Video Viewer aktualisiert die Bildschirmanzeige mit den Videodaten vom Server.

Full Screen (Gesamtanzeige)
Der Video Viewer verwendet den gesamten Client-Desktop für die Videoanzeige. Diese Option ist nur dann verfügbar, wenn der Video Viewer nicht im Gesamtanzeigemodus ausgeführt wird.

Windowed (Fenstermodus)
Der Video Viewer wechselt vom Gesamtanzeigemodus in den Fenstermodus. Diese Option ist nur dann verfügbar, während der Video Viewer im Gesamtanzeigemodus ausgeführt wird.

Fit (Eingepasst)
Der Video Viewer passt die Größe so an, dass der Zieldesktop vollständig und ohne zusätzliche Ränder oder Bildlaufleisten angezeigt werden kann. Der Client-Desktop muss groß genug sein, um das größenangepasste Fenster anzuzeigen.

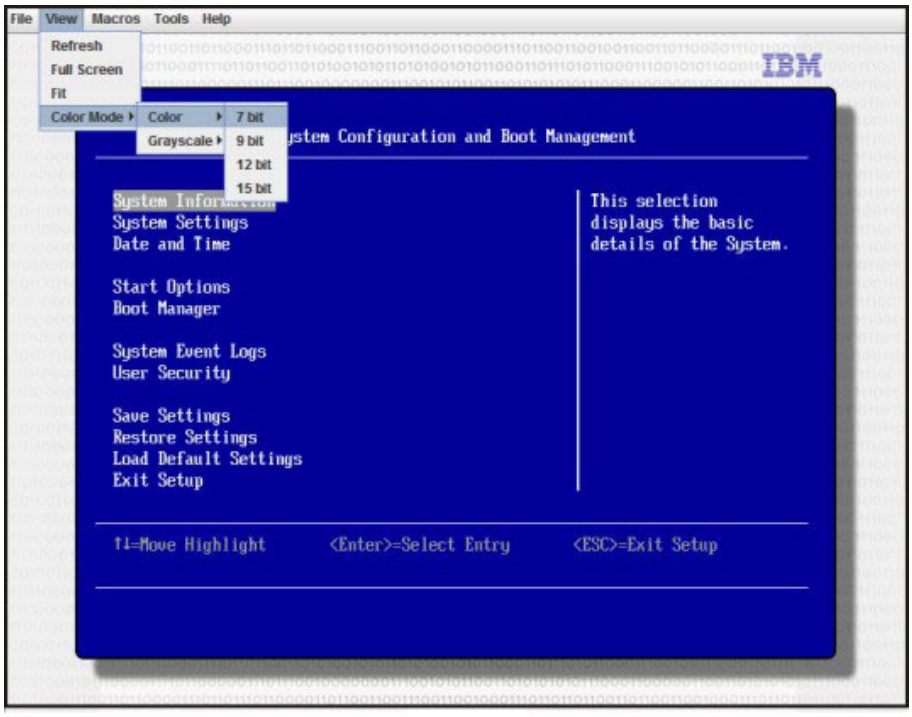
Fernsteuerung des Videofarbmodus

Wenn Ihre Verbindung zum fernen Server eine begrenzte Bandbreite hat, können Sie den Bandbreitenbedarf des Video Viewer verringern, indem Sie die Farbeinstellungen im Video Viewer-Fenster anpassen.

Anmerkung: Anstelle des Bandbreiten-Schiebereglers in der Schnittstelle von Remote Supervisor Adapter II hat das IMM eine Menüoption, die es ermöglicht, die Farbtiefe anzupassen, um bei geringer Bandbreite die übertragene Datenmenge zu verringern.

Gehen Sie wie folgt vor, um den Videofarbmodus zu ändern:

1. Klicken Sie im Fenster Video Viewer auf **View** (Ansicht).
2. Wenn Sie den Mauszeiger im Menü über **Color Mode** (Farbmodus) bewegen, werden zwei Farbmodusoptionen angezeigt:
   - Color (Farbe): 7, 9, 12 und 15-Bit
   - Grayscale (Graustufe): 16, 32, 64 und 128 Schattierungen

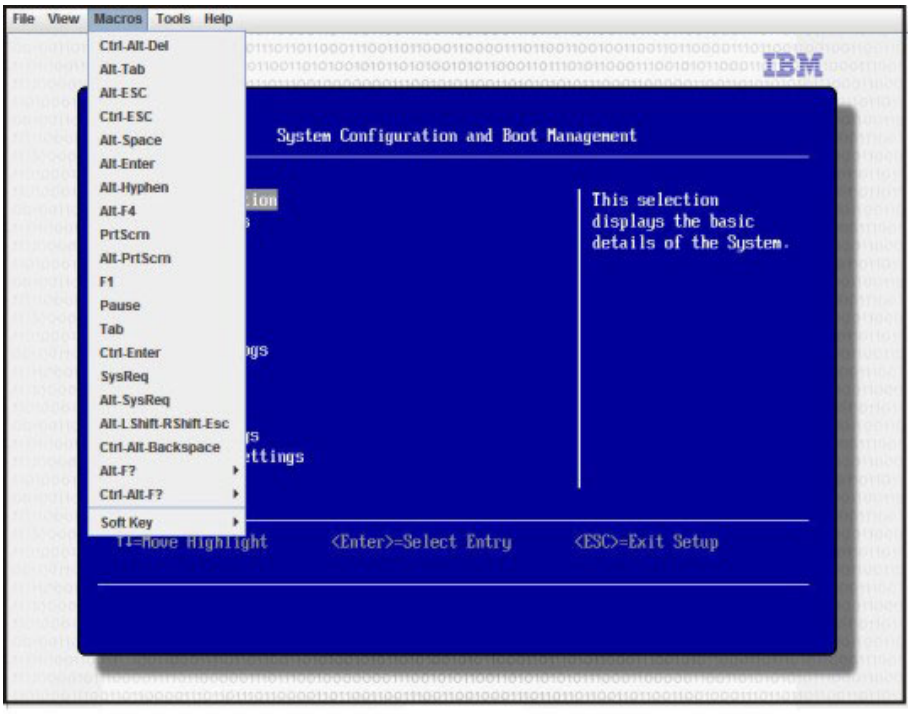


3. Wählen Sie die Farb- oder Graustufeneinstellung aus.

Tastaturunterstützung per Fernsteuerung

Das Betriebssystem auf dem Clientserver, den Sie verwenden, fängt bestimmte Tastenkombinationen ab, etwa "Strg + Alt + Entf" in Microsoft Windows, anstatt sie an den Blade-Server zu übertragen. Andere Tasten wie etwa F1 verursachen möglicherweise gleichzeitig eine Aktion auf dem Server und auf Ihrem Computer. Gehen Sie wie folgt vor, um Tastenkombinationen zu verwenden, die den fernen Server und nicht den lokalen Client beeinflussen:

1. Klicken Sie im Fenster Video Viewer auf **Macros**.
2. Wählen Sie eine der vordefinierten Tastenkombinationen aus dem Menü oder wählen Sie **Soft Key** (Programmfunktionssymbol), um benutzerdefinierte Tastenkombinationen auszuwählen oder hinzuzufügen.



Verwenden Sie die Menüoption **Macros** von Video Viewer, um spezielle Schaltflächen zu erstellen oder zu bearbeiten, mit deren Hilfe Tastatureingaben an den Server gesendet werden können.

Gehen Sie wie folgt vor, um spezielle Schaltflächen zu erstellen und zu bearbeiten:

1. Klicken Sie im Fenster "Video Viewer" auf **Macros**.
2. Wählen Sie **Soft Key** und dann **Add** (Hinzufügen). Ein neues Fenster wird geöffnet.
3. Klicken Sie auf **New**, um eine neue Tastenkombination hinzuzufügen, oder wählen Sie eine Tastenkombination und klicken Sie auf **Delete** (Löschen), um eine bestehende Tastenkombination zu entfernen.
4. Wenn Sie eine neue Kombination hinzufügen, geben Sie die Tastenkombination ein, die Sie im Dialogfenster definieren möchten, und klicken Sie dann auf **OK**.
5. Wenn Sie damit fertig sind, eine Tastenkombination zu definieren oder zu entfernen, klicken Sie auf **OK**.

Unterstützung für internationale Tastatur

Der Video Viewer verwendet plattformspezifischen nativen Code, um Tastaturereignisse abzufangen und direkt auf die Daten zur physischen Taste zuzugreifen. Der Client erkennt die Ereignisse der physischen Tasten und übergibt sie an den Server. Der Server erkennt dieselbe physische Tastatureingabe, die der Client festgestellt hat, und unterstützt alle Standardtastaturbelegungen. Die einzige Einschränkung dabei ist, dass das Ziel und der Client dieselbe Tastaturbelegung verwenden. Wenn ein ferner Benutzer eine andere Tastaturbelegung als der Server verwendet, kann der Benutzer die Serverbelegung umschalten, während der ferne Zugriff erfolgt, und anschließend wieder zurückschalten.

Tastaturdurchgriffsmodus

Die Tastaturdurchgriffsfunktion inaktiviert die Behandlung der meisten Sondertastenkombinationen auf dem Client, sodass sie direkt an den Server übergeben werden können. Dies bietet eine Alternative zur Verwendung der Makros.

Einige Betriebssysteme definieren bestimmte Tastatureingaben als außerhalb der Steuerung einer Anwendung, sodass das Verhalten des Durchgriffsmechanismus unabhängig vom Server ausgeführt wird. Beispiel: In einer Linux-Sitzung bewirkt die Tastenkombination Strg+Alt+F2 einen Wechsel zur virtuellen Konsole 2. Es gibt keinen Mechanismus, diese Tastenfolge abzufangen, und deshalb auch keine Möglichkeit für den Client, diese Tastatureingaben direkt an das Ziel zu übergeben. Die einzige Option in diesem Fall ist die Verwendung der Tastaturmakros, die für diese Zweck definiert wurden.

Gehen Sie wie folgt vor, um den Tastaturdurchgriffsmodus zu aktivieren oder zu inaktivieren:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Wählen Sie aus dem Menü **Session Options** (Sitzungsoptionen) aus.
3. Wenn das Fenster "Session Options" angezeigt wird, klicken Sie auf die Registerkarte **General** (Allgemein).
4. Wählen Sie das Kontrollkästchen **Pass all keystrokes to target** (Alle Tastatureingaben an Ziel übergeben) aus, um diese Funktion zu aktivieren oder zu inaktivieren.
5. Klicken Sie auf **OK**, um die Auswahl zu speichern.

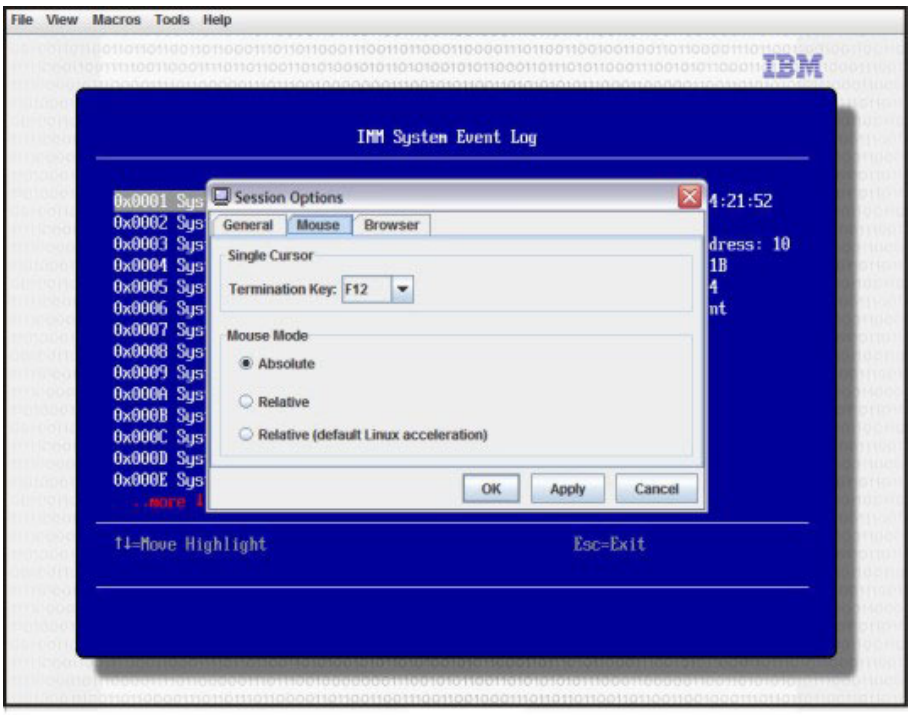
Mausunterstützung per Fernsteuerung

Im Fenster "Video Viewer" haben Sie verschiedene Möglichkeiten der Maussteuerung, einschließlich absolute Maussteuerung, relative Maussteuerung und Einzelcursormodus.

Absolute und relative Maussteuerung

Gehen Sie wie folgt vor, um auf die absoluten und relativen Optionen zum Steuern der Maus zuzugreifen:

1. Klicken Sie im Fenster "Remote Control" (Fernsteuerung) auf **Tools**.
2. Wählen Sie aus dem Menü **Session Options** (Sitzungsoptionen) aus.
3. Wenn das Fenster "Session Options" angezeigt wird, klicken Sie auf die Registerkarte **Mouse** (Maus).



4. Wählen Sie einen der folgenden Mausmodi aus:

   Absolute
   Der Client sendet Mauspositionsnachrichten an den Server, die immer relativ zum Ursprung (obere linke Ecke) des Anzeigebereichs sind.

   Relative
   Der Client sendet die Mausposition als relative Position im Hinblick auf die vorherige Position.

   Relative (default Linux acceleration) (Relativ (Linux-Standardbeschleunigung))
   Der Client wendet einen Beschleunigungsfaktor an, um die Maus besser auf Linux-Ziele abzustimmen. Die Beschleunigungseinstellungen wurden ausgewählt, um die Kompatibilität mit Linux-Distributionen zu maximieren.

Einzelcursormodus

Manche Betriebssysteme richten die lokalen und fernen Cursor nicht aneinander aus, was zu Abweichungen zwischen den lokalen und fernen Mauszeigern führt. Beim Einzelcursormodus wird der lokale Client ausgeblendet, während die Maus sich innerhalb des Video Viewer-Fensters befindet. Bei aktiviertem Einzelcursormodus sehen Sie nur den fernen Cursor.

Gehen Sie wie folgt vor, um den Einzelcursormodus zu aktivieren:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Wählen Sie **Single Cursor** (Einzelner Cursor) aus.

Wenn der Video Viewer im Einzelcursormodus läuft, können Sie die Maus nicht verwenden, um in ein anderes Fenster zu wechseln oder außerhalb des KVM-Clientfensters auf etwas zu klicken, da es keinen lokalen Cursor gibt. Klicken Sie zum Inaktivieren des Einzelcursormodus auf den festgelegten Beendigungsschlüssel.

Klicken Sie zum Anzeigen des festgelegten Beendigungsschlüssels oder zum Ändern des Beendigungsschlüssels auf **Tools > Session Options (Sitzungsoptionen) > Mouse**.

Ferne Steuerung der Stromversorgung

Vom Fenster "Video Viewer" können Sie Serverbefehle für Stromversorgung und Neustart versenden, ohne zum Web-Browser zurückzukehren. Gehen Sie wie folgt vor, um die Stromversorgung des Servers über den Video Viewer zu steuern:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Wenn Sie mit dem Mauszeiger im Menü auf **Power** (Stromversorgung) gehen, werden folgende Optionen angezeigt:

   On Schaltet die Stromversorgung des Servers ein.

   Off Schaltet die Stromversorgung des Servers aus.

   Reboot (Warmstart)
   Startet den Server erneut.

   Cycle (Aus- und wieder einschalten)
   Schaltet die Stromversorgung des Servers erst aus, dann wieder ein.

Leistungsstatistiken anzeigen

Gehen Sie wie folgt vor, um sich die "Video Viewer"-Leistungsstatistiken anzeigen zu lassen:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Klicken Sie auf **Stats** (Statistiken). Die folgenden Informationen werden angezeigt:

   Frame Rate (Vollbildrate)
   Ein gleitender Durchschnittswert der Anzahl an Bildern, die pro Sekunde durch den Client entschlüsselt wird.

   (Bandwidth) Bandbreite
   Ein gleitender Durchschnittswert der Gesamtzahl an Kilobytes pro Sekunde, die der Client empfängt.

   (Compression) Komprimierung
   Ein gleitender Durchschnittswert der Bandbreitenverkleinerung aufgrund von Videokomprimierung. Dieser Wert wird häufig mit 100.0% angegeben. Er wird auf ein Zehntel Prozent gerundet.

   (Packet Rate) Paketübertragungsrate
   Ein gleitender Durchschnittswert der Anzahl an Videopaketen, die pro Sekunde empfangen wird.

Remote Desktop Protocol starten

Wenn der Windows-basierte RDP-Client (Remote Desktop Protocol Client) installiert ist, können Sie einen RDP-Client anstelle des KVM-Clients verwenden. Der ferne Server muss so konfiguriert sein, dass er RDP-Verbindungen empfangen kann.

Ferner Datenträger

Im Fenster "Virtual Media Session" können Sie dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk oder ein USB-Flashlaufwerk auf Ihrem Computer zuordnen. Sie können auch ein Plattenimage auf Ihrem Computer angeben, das der Server verwenden soll. Sie können das Laufwerk für verschiedene Funktionen ver-

wenden, z. B. zum erneuten Starten (Booten) des Servers, zum Installieren neuer Software auf dem Server und zum Installieren oder Aktualisieren des Betriebssystems auf dem Server. Für den Zugriff auf den fernen Datenträger können Sie die Fernsteuerungsfunktion verwenden. Die Laufwerk und Plattenimages werden auf dem Server als USB-Laufwerke angezeigt.

Anmerkungen:

1. Die folgenden Serverbetriebssysteme bieten USB-Unterstützung, die für die Funktion für ferne Datenträger erforderlich ist:
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003
   - Red Hat Linux, Version 4.0 und 5.0
   - SUSE Linux Version 10.0
   - Novell NetWare 6.5
2. Für den Client-Server ist das Plug-in Java 1.5 oder eine aktuellere Version erforderlich.
3. Der Client-Server muss über einen Mikroprozessor vom Typ Intel Pentium III (oder neuer) mit 700 MHz oder mehr (oder über einen funktional entsprechenden Mikroprozessor) verfügen.

Zugriff auf die Fernsteuerung

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung zu starten und auf einen fernen Datenträger zuzugreifen:

1. Melden Sie sich am IMM an. Weitere Informationen hierzu finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Remote Control** (Fernsteuerung).
3. Klicken Sie auf der Seite "Remote Control" auf eine der folgenden Optionen für **Start Remote Control**:
   - Wenn Sie während Ihrer Sitzung exklusiven Fernzugriff möchten, klicken Sie auf **Start Remote Control in Single User Mode** (Fernsteuerung im Einzelbenutzermodus starten).
   - Wenn Sie möchten, dass während Ihrer Sitzung auch andere Benutzer auf die ferne Konsole (KVM) zugreifen können, klicken Sie auf **Start Remote Control in Multi-user Mode** (Fernsteuerung im Mehrbenutzermodus starten).

   Das Fenster "Video Viewer" wird geöffnet.
4. Um das Fenster "Virtual Media Session" zu öffnen, klicken Sie im Fenster "Video Viewer" auf **Tools** > **Launch Virtual Media** (Tools - Virtuelle Datenträger starten).

Anmerkung: Wenn vor dem Öffnen des Fensters "Remote Control" das Kontrollkästchen **Encrypt disk and KVM data during transmission** (Disketten- und KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Datenträgerdaten mit ADES verschlüsselt.
Das Fenster "Virtual Media Session" ist von dem Fenster "Video Viewer" getrennt. Im Fenster "Virtual Media Session" sind alle Laufwerke auf dem Client aufgelistet, die als ferne Laufwerke zugeordnet werden können. Im Fenster "Virtual Media Session" können Sie außerdem ISO-Image- und Diskettenimage-Dateien als virtuelle Laufwerke zuordnen. Jedes zugeordnete Laufwerk kann als schreibgeschützt gekennzeichnet werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt.

Laufwerkzuordnung mit IMM-Firmware-Version 1.03 und späteren Versionen festlegen und aufheben

Wählen Sie zum Zuordnen eines Laufwerks das Kontrollkästchen **Select** (Auswählen) neben dem Laufwerk aus, das Sie zuordnen möchten.

Anmerkung: Ein CD- oder DVD-Laufwerk muss Datenträger enthalten, bevor es zugeordnet wird. Wenn das Laufwerk leer ist, werden Sie aufgefordert, eine CD oder eine DVD in das Laufwerk einzulegen.

Klicken Sie auf die Schaltfläche **Mount Selected** (Auswahl anhängen), um das ausgewählte Laufwerk bzw. die ausgewählten Laufwerke anzuhängen oder und zuzuordnen.

Wenn Sie auf **Add Image** (Bild hinzufügen) klicken, können Disketten- und ISO-Imagedateien zur Liste verfügbarer Laufwerke hinzugefügt werden. Wenn die Disketten- oder ISO-Imagedatei im Fenster "Virtual Media Session" angeführt wird, kann sie genau wie die anderen Laufwerke zugeordnet werden.

Klicken Sie zum Aufheben der Laufwerkzuordnung auf die Schaltfläche **Unmount All** (Alle abhängen). Bevor die Laufwerkzuordnungen aufgehoben werden, müssen Sie Ihren Wunsch bestätigen, dass die Laufwerkzuordnungen aufgehoben werden sollen.

Anmerkung: Nachdem Sie bestätigt haben, dass die Laufwerkzuordnungen aufgehoben werden sollen, werden sämtliche Laufwerke abgehängt. Sie können Laufwerke nicht einzeln abhängen.

Sie können eine Diskettenimagedatei auswählen und das Diskettenimage auf dem IMM-Speicher speichern. So kann die Festplatte an den Server angehängt bleiben, sodass Sie später Zugriff auf die Festplatte haben, auch nachdem die IMM-Webschnittstellensitzung beendet wurde. Maximal ein Datenträgerimage kann auf der IMM-Karte gespeichert werden. Der Inhalt des Laufwerks oder des Image darf 1,44 MB nicht überschreiten. Gehen Sie wie folgt vor, um eine Diskettenimagedatei hochzuladen:

1. Klicken Sie auf **RDOC**.
2. Wenn das neue Fenster geöffnet wird, klicken Sie auf **Upload**.
3. Klicken Sie auf **Browse** (Durchsuchen), um die Imagedatei auszuwählen, die Sie verwenden möchten.
4. Geben Sie im Feld **Name** einen Namen für das Image ein und klicken Sie auf **OK**, um die Datei hochzuladen.

   Anmerkung: Wählen Sie zum Löschen der Imagedatei aus dem Speicher den Namen im Fenster "RDOC Setup" (RDOC-Konfiguration) und klicken Sie auf **Delete** (Löschen).

Laufwerkzuordnung mit IMM-Firmware-Version 1.02 und früheren Versionen festlegen und aufheben

Wählen Sie zum Zuordnen eines Laufwerks das Kontrollkästchen **Mapped** (Zugeordnet) neben dem Laufwerk aus, das Sie zuordnen möchten.

Anmerkung: Ein CD- oder DVD-Laufwerk muss Datenträger enthalten, bevor es zugeordnet wird. Wenn das Laufwerk leer ist, werden Sie aufgefordert, eine CD oder eine DVD in das Laufwerk einzulegen.

Wenn Sie auf **Add Image** (Bild hinzufügen) klicken, können Disketten- und ISO-Imagedateien zur Liste verfügbarer Laufwerke hinzugefügt werden. Wenn die Disketten- oder ISO-Imagedatei im Fenster "Virtual Media Session" angeführt wird, kann sie genau wie die anderen Laufwerke zugeordnet werden.

Wählen Sie zum Aufheben einer Laufwerkzuordnung das Kontrollkästchen **Mapped** für das Laufwerk ab. Bevor die Laufwerkzuordnung aufgehoben wird, müssen Sie Ihren Wunsch bestätigen, dass die Laufwerkzuordnung aufgehoben werden soll.

Sie können eine Diskettenimagedatei auswählen und das Diskettenimage auf dem IMM-Speicher speichern. So kann die Festplatte an den Server angehängt bleiben, sodass Sie später Zugriff auf die Festplatte haben, auch nachdem die IMM-Webschnittstellensitzung beendet wurde. Maximal ein Datenträgerimage kann auf der IMM-Karte gespeichert werden. Der Inhalt des Laufwerks oder des Image darf 1,44 MB nicht überschreiten. Gehen Sie wie folgt vor, um eine Diskettenimagedatei hochzuladen:

1. Klicken Sie auf **RDOC**.
2. Wenn das neue Fenster geöffnet wird, klicken Sie auf **Upload**.
3. Klicken Sie auf **Browse**, um die Imagedatei auszuwählen, die Sie verwenden möchten.
4. Geben Sie im Feld **Name** einen Namen für das Image ein und klicken Sie auf **OK**, um die Datei hochzuladen.

   Anmerkung: Wählen Sie zum Löschen der Imagedatei aus dem Speicher den Namen im Fenster "RDOC Setup" (RDOC-Konfiguration) und klicken Sie auf **Delete**.

Fernsteuerung beenden

Schließen Sie die Fenster "Video Viewer" und "Virtual Media Session", wenn Sie die Verwendung der Fernsteuerungsfunktion beenden möchten.

PXE-Netzboot einrichten

Wenn Sie Ihren Server für den Versuch eines PXE-Netzboots (Preboot Execution Environment) beim nächsten Serverneustart konfigurieren möchten, gehen Sie wie folgt vor:

1. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **PXE Network Boot**.
3. Wählen Sie das Kontrollkästchen **Attempt PXE network boot at next server restart** (Bei nächstem Serverneustart PXE-Netzboot versuchen) aus.
4. Klicken Sie auf **Save**.

Firmware aktualisieren

Verwenden Sie die Option "Firmware Update" im Navigationsfenster, um die IMM-Firmware, die Server-Firmware für System x oder die Firmware für Dynamic System Analysis (DSA) zu aktualisieren.

Gehen Sie wie folgt vor, um die Firmware zu aktualisieren.

Anmerkung: Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die tatsächliche Vorgehensweise weicht möglicherweise geringfügig von der Beschreibung im vorliegenden Dokument ab.

1. Laden Sie die aktuelle Firmwareaktualisierung herunter, die dem Server entspricht, auf dem das IMM installiert ist:
   a. Öffnen Sie http://www.ibm.com/systems/support/.
   b. Klicken Sie unter **Product support** (Produktunterstützung) entweder auf **System x** oder auf **BladeCenter**.
   c. Klicken Sie unter **Popular links** (Häufig genutzte Links) auf **Software and device drivers** (Software und Einheitentreiber).
   d. Klicken Sie auf den für Ihren Server gültigen Link, um die Matrix mit herunterladbaren Dateien anzuzeigen.
   e. Blättern Sie zum Bereich IMM, Server-Firmware oder DSA, wählen Sie den Link für die Firmwareaktualisierung und speichern Sie die Aktualisierungsdatei.
2. Melden Sie sich am IMM an. Weitere Informationen finden Sie in Kapitel 2, „IMM-Webschnittstelle öffnen und verwenden", auf Seite 13.
3. Klicken Sie im Navigationsfenster auf **Firmware Update**.
4. Klicken Sie auf **Browse** (Durchsuchen).
5. Navigieren Sie zum Aktualisierungspaket, das Sie aktualisieren möchten.

   Anmerkung:
   a. Die Server-Firmware für System x kann nicht aktualisiert werden, während der Server ausgeschaltet ist oder gestartet wird.
   b. Informationen dazu, welchen Firmwaretyp Sie verwenden sollten, finden Sie in der Readme-Datei des Aktualisierungspakets. In den meisten Fällen kann das IMM entweder die EXE- oder die BIN-Datei verwenden, um die Aktualisierung durchzuführen.
6. Klicken Sie auf **Open**. Die Datei wird (einschließlich des vollständigen Pfads) im Feld neben **Browse** angezeigt.
7. Klicken Sie zum Starten des Aktualisierungsprozesses auf **Update**. Eine Statusanzeige wird geöffnet, während die Datei auf den temporären Speicher des IMM übertragen wird. Ein Bestätigungsfenster wird geöffnet, wenn die Datei fertig übertragen ist.
8. Überprüfen Sie, ob es sich bei der im Fenster "Confirm Firmware Update" (Firmwareaktualisierung bestätigen) angezeigten Datei um die handelt, die Sie aktualisieren möchten. Sollte dies nicht der Fall sein, klicken Sie auf **Cancel** (Abbrechen).
9. Klicken Sie zum Abschließen des Aktualisierungsprozesses auf **Continue** (Fortfahren). Eine Statusanzeige öffnet sich, während die Firmware aktualisiert wird. Ein Bestätigungsfenster öffnet sich mit der Meldung, dass die Aktualisierung erfolgreich war.
10. Zum Aktualisieren der IMM-Firmware klicken Sie im Navigationsfenster auf **Restart IMM** und dann auf **Restart**. Bei Aktualisierungen der Server-Firmware für System x und von DSA ist es nicht erforderlich, das IMM erneut zu starten. Diese Aktualisierungen werden wirksam, wenn der Server das nächste Mal gestartet wird.
11. Klicken Sie auf **OK**, um zu bestätigen, dass Sie das IMM erneut starten möchten.
12. Klicken Sie auf **OK**, um das aktuelle Browserfenster zu schließen.

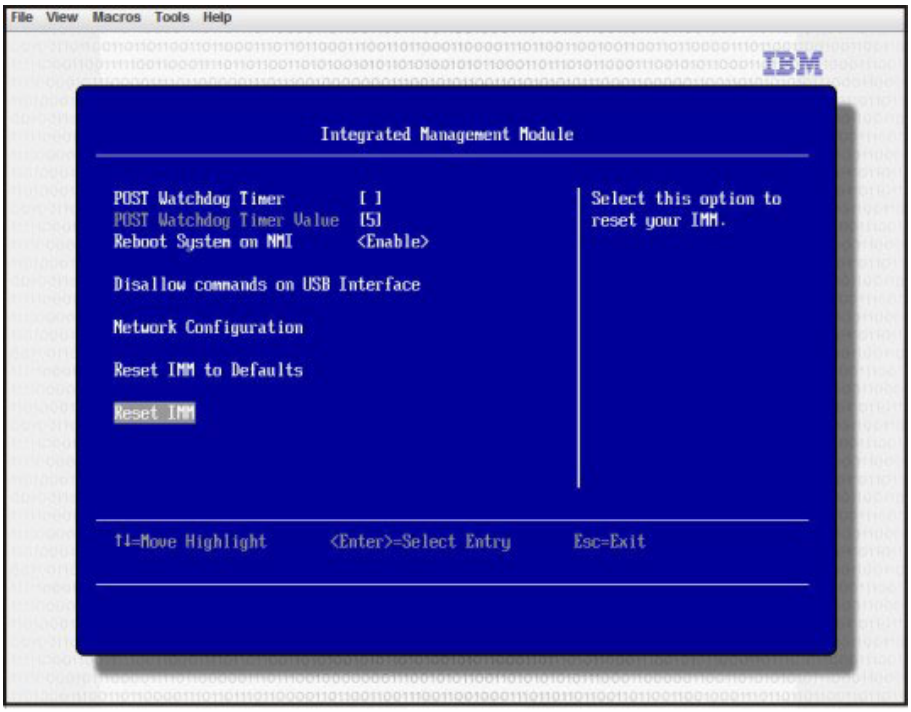
13. Melden Sie sich nach dem IMM-Neustart erneut am IMM an, um auf die Webschnittstelle zuzugreifen.

IMM mit Konfigurationsdienstprogramm zurücksetzen

Gehen Sie wie folgt vor, um das IMM über das Konfigurationsdienstprogramm zurückzusetzen:

1. Schalten Sie den Server ein.

   Anmerkung: Der Netzschalter wird etwa 2 Minuten nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.
2. Wenn die Aufforderung `F1 Setup` (F1-Konfiguration) angezeigt wird, drücken Sie F1. Wenn Sie sowohl ein Startkennwort als auch ein Administratorkennwort festgelegt haben, müssen Sie das Administratorkennwort eingeben, um auf das vollständige Menü des Konfigurationsdienstprogramms zugreifen zu können.
3. Wählen Sie im Hauptmenü des Konfigurationsdienstprogramms **System Settings** (Systemeinstellungen) aus.
4. Wählen Sie in der nächsten Anzeige die Option **Integrated Management Module** aus.
5. Wählen Sie **Reset IMM** (IMM zurücksetzen).



Anmerkung: Nachdem Sie das IMM zurückgesetzt haben, wird sofort diese Bestätigungsnachricht angezeigt:

```
IMM reset command has been sent successfully (Befehl zum Zurücksetzen des IMM
wurde erfolgreich gesendet)!! Press ENTER to continue (Zum Fortfahren Eingabetaste drücken).
```

Der IMM-Rücksetzvorgang ist noch nicht fertig. Sie müssen etwa 4 Minuten warten, bis das IMM zurückgesetzt ist, bevor das IMM wieder funktioniert. Wenn Sie während des Rücksetzvorgangs des Servers versuchen, auf Firmwa-

redaten zuzugreifen, wird in den Feldern Unknown (Unbekannt) angezeigt und die Beschreibung lautet Error retrieving information from IMM (Fehler beim Abrufen von Informationen vom IMM).

Tools und Dienstprogramme mit IMM- und Server-Firmware für IBM System x verwalten

In diesem Abschnitt werden die Tools und Dienstprogramme beschrieben, die von der IMM- und der Server-Firmware für IBM System x unterstützt werden. Für die IBM Tools für die Verwaltung von IMM-Inband-Prozessen müssen keine Einheitentreiber installiert werden. Wenn Sie jedoch bestimmte Tools in Inband-Prozessen verwenden möchten, wie z. B. IPMItool, müssen Sie die OpenIPMI-Treiber installieren.

Aktualisierungen und Downloads für IBM Systemmanagementtools und -Dienstprogramme sind auf der IBM Website verfügbar. Gehen Sie wie folgt vor, um nach Aktualisierungen für Tools und Dienstprogramme zu suchen.

Anmerkung: Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die Vorgehensweisen zum Bestimmen der Firmware und der Dokumentation weicht möglicherweise geringfügig von den Beschreibungen im vorliegenden Dokument ab.

1. Öffnen Sie http://www.ibm.com/systems/support/.
2. Klicken Sie unter **Product support** (Produktunterstützung) auf **System x**.
3. Klicken Sie unter **Popular links** auf den Eintrag **Utilities**.

IPMItool verwenden

IPMItool bietet diverse Tools, die Sie zum Verwalten und Konfigurieren eines IPMI-Systems verwenden können. Sie können IPMItool intern oder extern verwenden, um das IMM zu verwalten und zu konfigurieren.

Gehen Sie für weitere Informationen zu IPMItool oder zum Herunterladen von IPMItool auf http://sourceforge.net/.

OSA System Management Bridge verwenden

OSA System Management Bridge (SMBridge) ist ein Werkzeug, mit dessen Hilfe Server über Fernzugriff verwaltet werden können. Sie können es verwenden, um Server mithilfe von Protokollen von IPMI 1.5 und Serial over LAN (SOL) zu verwalten.

Weitere Informationen zu SMBridge finden Sie unter http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-62198&brandind=5000008 oder gehen Sie wie folgt vor:

1. Gehen Sie auf http://www.ibm.com/systems/support/.
2. Klicken Sie auf **System x**.
3. Klicken Sie unter **Support & downloads** (Unterstützung und Downloads) auf **Search** (Suche).
4. Geben Sie in das Suchfeld smbridge ein und klicken Sie auf **Search**.
5. Klicken Sie in der Ergebnisliste auf den Link **SMBridge Tool Help - Servers**.

Dienstprogramm für erweiterte Einstellungen verwenden

Zum Verwalten des IMM ist IBM Advanced Settings Utility (ASU) ab Version 3.0.0 erforderlich. ASU ist ein Werkzeug, das Sie verwenden können, um von der Befehlszeilenschnittstelle aus auf mehreren Betriebssystemplattformen Firmware-Einstellungen zu ändern. Sie können damit auch ausgewählte IMM-Konfigurationsbefehle ausgeben. Sie können ASU intern oder extern verwenden, um das IMM zu verwalten und zu konfigurieren.

Anmerkung: Wenn die USB-Inband-Schnittstelle (LAN over USB) inaktiviert ist, ist für ASU die Installation von IPMI-Einheitentreibern erforderlich.

Weitere Informationen finden Sie unter http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55021&brandind=5000008 oder gehen Sie wie folgt vor:

1. Gehen Sie auf http://www.ibm.com/systems/support/.
2. Klicken Sie auf **System x**, wählen Sie Ihren Server aus dem Menü **Product family** und klicken Sie auf **Go**.
3. Wählen Sie im Menü **Refine results** (Ergebnisse eingrenzen) **Advanced Settings Utility** aus und klicken Sie auf **Go**.
4. Klicken Sie auf den Link zur aktuellen Version des ASU.

IBM Flashdienstprogramme verwenden

Ein Flashdienstprogramm ermöglicht das Aktualisieren von Hardware und Server-Firmware, sodass neue Firmware oder Firmwareaktualisierungen nicht manuell von einem physischen Datenträger oder einem anderen Medium installiert werden müssen. Sie können IBM Flashdienstprogramme entweder intern oder extern für IMM, Server-Firmware und DSA verwenden. Gehen Sie wie folgt vor, um ein Flashdienstprogramm zu finden:

1. Gehen Sie auf http://www.ibm.com/systems/support/.
2. Klicken Sie unter **Product support** (Produktunterstützung) auf **System x**.
3. Geben Sie in das Suchfeld `flash utility` (Flashdienstprogramm) ein und klicken Sie auf **Search** (Suche).
4. Klicken Sie auf den Link zum entsprechenden Flashdienstprogramm.

Andere Verwaltungsmethoden für das IMM

Mit den folgenden Benutzerschnittstellen können Sie das IMM verwalten und konfigurieren:

- IMM-Webschnittstelle
- SNMPv1
- SNMPv3
- Telnet-Befehlszeilenschnittstelle
- SSH-Befehlszeilenschnittstelle

Kapitel 6. LAN over USB

Im Gegensatz zum BMC und zum Remote Supervisor Adapter II erfordert das IMM keine IPMI-Einheitentreiber oder USB-Dämonen für die Inband-IMM-Kommunikation. Stattdessen ermöglicht eine Schnittstelle "LAN over USB" die Inband-Kommunikation mit dem IMM. Die IMM-Hardware auf der Systemplatine zeigt einen internen Ethernet-Netzschnittstellencontroller vom IMM zum Betriebssystem an.

Anmerkung: LAN over USB wird in der IMM-Webschnittstelle auch als „USB-Inband-Schnittstelle” bezeichnet.

Als IMM-IP-Adresse für die Schnittstelle "LAN over USB" ist die statische Adresse 169.254.95.118 mit der Teilnetzmaske 255.255.0.0 eingestellt. Die einzige Ausnahme besteht für das IMM im Sekundärknoten in einem System mit mehreren Knoten (z. B. x3850 X5 oder x3950 X5). Hier ist die IMM-seitige IP-Adresse der Schnittstelle "LAN over USB" 169.254.96.118.

Potenzielle Konflikte mit der Schnittstelle "LAN over USB"

In manchen Situationen können Konflikte zwischen der Schnittstelle "LAN over USB" des IMM und bestimmten Netzkonfigurationen, Anwendungen oder beidem auftreten. So versucht Open MPI beispielsweise, alle verfügbaren Netzschnittstellen auf einem Server zu verwenden. Open MPI erkennt die Schnittstelle "LAN over USB" des IMM und versucht, diese für die Kommunikation mit anderen Systemen in einer Clusterumgebung zu verwenden. Die Schnittstelle "LAN over USB" ist eine interne Schnittstelle und eignet sich daher nicht für die externe Kommunikation mit anderen Systemen im Cluster.

Konflikte mit der IMM-Schnittstelle "LAN over USB" lösen

Es gibt mehrere Maßnahmen, mit denen Konflikte zwischen der Schnittstelle "LAN over USB" und Netzkonfigurationen und -anwendungen gelöst werden können:

- Konfigurieren Sie die Anwendung bei Konflikten mit Open MPI so, dass sie nicht versucht, die Schnittstelle zu verwenden.
- Inaktivieren Sie die Schnittstelle (führen Sie unter Linux den Befehl `ifdown` aus).
- Entfernen Sie den Einheitentreiber (führen Sie unter Linux den Befehl `rmmod` aus).
- Inaktivieren Sie die USB-Inband-Schnittstelle im IMM mit einer der folgenden Methoden.

  Wichtiger Hinweis: Wenn Sie die USB-Inband-Schnittstelle inaktivieren, können Sie keine Inbandaktualisierung der IMM-Firmware mithilfe der Linux- oder Windows-Flashdienstprogramme durchführen. Wenn die USB-Inband-Schnittstelle inaktiviert ist, verwenden Sie die Option "Firmware Update" auf der IMM-Webschnittstelle zum Aktualisieren der Firmware. Weitere Informationen finden Sie im Abschnitt „Firmware aktualisieren” auf Seite 137.

  Wenn Sie die USB-Inband-Schnittstelle inaktivieren, inaktivieren Sie auch die Watchdog-Zeitlimitüberschreitungen, um zu verhindern, dass der Server unerwartet neu startet. Weitere Informationen zum Inaktivieren der Watchdogs finden Sie unter „Serverzeitlimits festlegen” auf Seite 23.

– Informationen zur Inaktivierung der Schnittstelle "LAN over USB" über die IMM-Webschnittstelle finden Sie unter „USB-Inband-Schnittstelle inaktivieren” auf Seite 26.
– Zum Inaktivieren der Schnittstelle "LAN over USB" über die Webschnittstelle des erweiterten Managementmoduls gehen Sie wie folgt vor:
  1. Melden Sie sich an der Webschnittstelle des erweiterten Managementmoduls an.
  2. Klicken Sie im Navigationsfenster unter der Überschrift **Blade Tasks** (Blade-Aufgaben) auf **Blade Configuration** (Blade-Konfiguration).
  3. Blättern Sie abwärts zur Serviceprozessor-Schnittstelle "LAN over USB" auf der Webseite für die Blade-Konfiguration. In diesem Abschnitt werden alle Blade-Server im Gehäuse aufgelistet, auf denen die Schnittstelle "LAN over USB" aktiviert und inaktiviert werden kann.
  4. Aktivieren Sie die Kontrollkästchen neben den Blade-Servern, die aktiviert oder inaktiviert werden sollen.
  5. Klicken Sie auf die Schaltfläche **Disable** (Inaktivieren), um die Schnittstelle "LAN over USB" auf den ausgewählten Blade-Servern zu inaktivieren.

Die Schnittstelle "LAN over USB" manuell konfigurieren

Damit das IMM die Schnittstelle "LAN over USB" verwenden kann, müssen Sie möglicherweise andere Konfigurationstasks abschließen, wenn die automatische Konfiguration fehlschlägt oder wenn Sie es vorziehen, "LAN over USB" manuell einzurichten. Das Firmwareaktualisierungspaket oder das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility) versucht, die Konfiguration automatisch durchzuführen. Weitere Informationen zur Konfiguration von "LAN over USB" auf verschiedenen Betriebssystemen finden Sie im IBM White Paper *Transitioning to UEFI and IMM* auf der IBM Website.

Einheitentreiber installieren

Damit das IMM die Schnittstelle "LAN over USB" verwenden kann, müssen Sie möglicherweise Betriebssystemtreiber installieren. Wenn die automatische Konfiguration fehlschlägt oder wenn Sie LAN over USB lieber manuell konfigurieren möchten, verwenden Sie eine der folgenden Vorgehensweisen. Weitere Informationen zur Konfiguration von "LAN over USB" auf verschiedenen Betriebssystemen finden Sie im IBM White Paper *Transitioning to UEFI and IMM* auf der IBM Website.

Windows IPMI-Einheitentreiber installieren

Der Microsoft IPMI-Einheitentreiber wird auf Microsoft Windows Server 2003 R2-Betriebssystemen nicht standardmäßig installiert. Gehen Sie wie folgt vor, um den Microsoft IPMI-Einheitentreiber zu installieren:

1. Klicken Sie im Windows-Desktop auf **Start > Control Panel (Steuerkonsole) > Add or Remove Programs (Programme hinzufügen oder entfernen)**.
2. Klicken Sie auf **Add/Remove Windows Components** (Windows-Komponenten hinzufügen/entfernen).
3. Wählen Sie aus der Komponentenliste **Management and Monitoring Tools** (Verwaltung- und Überwachungstools) aus und klicken Sie dann auf **Details**.
4. Wählen Sie **Hardware Management** aus.
5. Klicken Sie auf **Next**. Der Installationsassistent wird geöffnet und führt Sie durch die Installation.

   Anmerkung: Möglicherweise ist die Windows-Installations-CD erforderlich.

Windows-Einheitentreiber für LAN over USB installieren

Wenn Sie Windows installieren, wird im Gerätemanager eine unbekannte RNDIS-Einheit angezeigt. Sie müssen eine Windows-INF-Datei installieren, die diese Einheit bestimmt und vom Windows-Betriebssystem zum Erkennen und Verwenden der LAN over USB-Funktion benötigt wird. Die signierte Version der INF-Datei ist in allen Windows-Versionen der IMM-, UEFI- und DSA-Aktualisierungspakete enthalten. Die Datei muss nur einmal installiert werden. Gehen Sie wie folgt vor, um die Windows-INF-Datei zu installieren:

1. Fordern Sie eine Windows-Version des IMM-, Server-Firmware- oder DSA-Aktualisierungspakets an (weitere Informationen finden Sie unter „Firmware aktualisieren" auf Seite 137).
2. Extrahieren Sie die Dateien `ibm_rndis_server_os.inf` und `device.cat` aus dem Firmware-Aktualisierungspaket, und kopieren Sie sie in das Unterverzeichnis `\WINDOWS\inf`.
3. **Für Windows 2003**: Installieren Sie die Datei `ibm_rndis_server_os.inf`, indem Sie mit der rechten Maustaste auf die Datei klicken und **Install** auswählen. Dadurch wird unter `\WINDOWS\inf` eine PNF-Datei mit demselben Namen erstellt. **Für Windows 2008**: Wählen Sie **Computer Management** (Computerverwaltung) und anschließend **Device Manager** (Gerätemanager) aus und suchen Sie die RNDIS-Einheit. Wählen Sie **Eigenschaften > Treiber > Treiber erneut installieren** aus. Verweisen Sie den Server auf das Verzeichnis `\Windows\inf`, in dem er die Datei `ibm_rndis_server_os.inf` finden und die Einheit installieren kann.
4. Wählen Sie **Computer Management** und anschließend **Device Manager** aus, klicken Sie mit der rechten Maustaste auf **Network adapters** und wählen Sie **Scan for hardware changes** (Nach geänderter Hardware suchen) aus. In einer Nachricht wird bestätigt, dass die Ethernet-Einheit gefunden und installiert wurde. Der Assistent für neue Hardware wird automatisch gestartet.
5. Wenn die Systemanfrage `Can Windows connect to Windows Update to search for software?` (Kann Windows eine Verbindung zu Windows Update herstellen, um nach Software zu suchen?) angezeigt wird, klicken Sie auf **No, not this time** (Nein, diesmal nicht). Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.
6. Wenn die Systemanfrage `What do you want the wizard to do?` (Was soll der Assistent tun?) angezeigt wird, klicken Sie auf **Install from a list or specific location (Advanced)** (Aus einer Liste oder bestimmten Position installieren (Erweitert)). Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.
7. Wenn die Aufforderung `Please choose your search and installation options` (Bitte wählen Sie Ihre Such- und Installationsoptionen aus) angezeigt wird, klicken Sie auf **Don't search. I will choose the driver to install** (Nicht suchen. Ich werde den zu installierenden Treiber auswählen). Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.
8. Wenn die Aufforderung `Select a hardware type, and then click Next` (Einen Hardwaretyp auswählen, dann auf "Next" klicken) angezeigt wird, klicken Sie auf **Network adapters**. Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.
9. Wenn die Anzeige `Completing the Found New Hardware Wizard` (Gefundener Assistent für neue Hardware wird fertiggestellt) erscheint, klicken Sie auf **Finish** (Fertigstellen).

Anmerkung: Es wird eine neue LAN-Verbindung und möglicherweise eine Nachricht wie die folgende angezeigt: `This connection has limited or no connectivity` (Diese Verbindung verfügt nur über eingeschränkte oder keine Konnektivität). Ignorieren Sie diesen Hinweis.

10. Wechseln Sie zurück zum Gerätemanager. Überprüfen Sie, ob unter **Network Adapters** die Option **IBM USB Remote NDIS Device** (IBM USB RNDIS-Netzeinheit) angezeigt wird.
11. Öffnen Sie eine Eingabeaufforderung, geben Sie `ipconfig` ein, und drücken Sie die Eingabetaste. Die LAN-Verbindung für die IBM USB RNDIS-Einheit wird mit einer IP-Adresse im Bereich von 169.254.*xxx.xxx* mit einer auf 255.255.0.0 eingestellten Teilnetzmaske angezeigt.

Linux-Einheitentreiber für LAN over USB installieren

Aktuelle Linux-Versionen wie z. B. RHEL5 Update 2 und SLES10 Service Pack 2 unterstützen standardmäßig die Schnittstelle "LAN over USB". Diese Schnittstelle wird während der Installation dieser Betriebssysteme erkannt und angezeigt. Verwenden Sie beim Konfigurieren der Einheit die statische IP-Adresse 169.254.95.130 mit der Teilnetzmaske 255.255.0.0.

Anmerkung: Ältere Linux-Varianten erkennen die Schnittstelle "LAN over USB" möglicherweise nicht und erfordern möglicherweise eine manuelle Konfiguration. Informationen zur Konfiguration von LAN over USB auf bestimmten Linux-Varianten finden Sie im IBM White Paper *Transitioning to UEFI and IMM* (Statusänderung auf UEFI und IMM) auf der IBM Website.

Die Schnittstelle "LAN over USB" des IMM erfordert das Laden der Einheitentreiber `usbnet` und `cdc_ether`. Wenn die Einheitentreiber nicht installiert wurden, verwenden Sie den Befehl "modprobe", um sie zu installieren. Wenn diese Einheitentreiber installiert sind, wird die USB-Netzschnittstelle des IMM als Netzeinheit im Betriebssystem angezeigt. Um zu erkennen, welchen Namen das Betriebssystem der USB-Netzschnittstelle des IMM zugewiesen hat, geben Sie Folgendes ein:

```
dmesg | grep -i cdc ether
```

Verwenden Sie den Befehl "ifconfig", um die Schnittstelle so zu konfigurieren, dass sie über eine IP-Adresse im Bereich 169.254.*xxx.xxx* verfügt. Beispiel:

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

Diese Schnittstelle ist so konfiguriert, dass sie jedes Mal, wenn das Betriebssystem gestartet wird, über eine IP-Adresse im Bereich 169.254.*xxx.xxx* verfügt.

Kapitel 7. Befehlszeilenschnittstelle

Verwenden Sie die IMM-Befehlszeilenschnittstelle (CLI) für den Zugriff auf IMM, ohne die Webschnittstelle verwenden zu müssen. Diese Schnittstelle stellt einen Teil der Managementfunktionen bereit, die von der Webschnittstelle bereitgestellt werden.

Sie können über eine Telnet- oder eine SSH-Sitzung auf die Befehlszeilenschnittstelle zugreifen. Bevor Sie CLI-Befehle absetzen können, müssen Sie durch das IMM authentifiziert worden sein.

IMM mit IPMI verwalten

Anfangs ist beim IMM die Benutzer-ID 2 auf den Benutzernamen "USERID" und das Kennwort "PASSW0RD" (mit einer Null anstelle des Buchstaben "O") eingestellt. Dieser Benutzer hat Administratorzugriff.

Wichtiger Hinweis: Ändern Sie für größere Sicherheit dieses Standardkennwort bei der Erstkonfiguration.

Das IMM bietet außerdem die folgenden IPMI-Funktionen (Intelligent Peripheral Management Interface) zur Verwaltung ferner Server:

Befehlszeilenschnittstellen
Die Befehlszeilenschnittstelle gewährt durch das IPMI 2.0-Protokoll direkten Zugriff auf Serververwaltungsfunktionen. Sie können SMBridge oder IPMItool verwenden, um Befehle zum Steuern der Stromversorgung am Server, zum Anzeigen von Serverinformationen und zum Identifizieren des Servers auszugeben. Mit SMBridge können Sie außerdem einen oder mehrere Befehle in einer Textdatei speichern und diese Datei als Script ausführen. Weitere Informationen zu IPMItool finden Sie im Abschnitt „IPMItool verwenden" auf Seite 140. Weitere Informationen zu SMBridge finden Sie im Abschnitt „OSA System Management Bridge verwenden" auf Seite 140.

Serial over LAN
Verwenden Sie zum Verwalten von Servern von einem fernen Standort aus SMBridge oder IPMItool, um eine SOL-Verbindung (Serial over LAN) herzustellen. Weitere Informationen zu IPMItool finden Sie im Abschnitt „IPMItool verwenden" auf Seite 140. Weitere Informationen zu SMBridge finden Sie im Abschnitt „OSA System Management Bridge verwenden" auf Seite 140.

Zugriff auf die Befehlszeile

Um auf die Befehlszeile zuzugreifen, starten Sie eine Telnet- oder SSH-Sitzung mit der IP-Adresse des IMM (weitere Informationen hierzu finden Sie im Abschnitt „Seriell-zu-Telnet- oder SSH-Umleitung konfigurieren" auf Seite 39).

Anmeldung an der Befehlszeilensitzung

Gehen Sie wie folgt vor, um sich an der Befehlszeile anzumelden:

1. Stellen Sie eine Verbindung mit dem IMM her.

2. Wenn Sie nach dem Benutzernamen gefragt werden, geben Sie die Benutzer-ID ein.
3. Wenn Sie nach dem Kennwort gefragt werden, geben Sie das Kennwort ein, das Sie zur Anmeldung am IMM verwenden.

   Sie werden an der Befehlszeile angemeldet. Die Befehlszeilenaufforderung lautet `system>`. Die Befehlszeilensitzung wird aufrechterhalten, bis Sie in der Befehlszeile `exit` (Verlassen) eingeben. Dann werden Sie abgemeldet und die Sitzung wird beendet.

Befehlssyntax

Lesen Sie die folgenden Richtlinien, bevor Sie die Befehle verwenden:

- Jeder Befehl weist das folgende Format auf:

  `Befehl [`*`Argumente`*`] [-`*`Optionen`*`]`
- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Der Befehlsname wird in Kleinbuchstaben angegeben.
- Alle Argumente müssen direkt auf den Befehl folgen. Die Optionen wiederum folgen direkt auf die Argumente.
- Vor jeder Option steht ein Bindestrich (-). Eine Option kann als Kurzoption (ein einzelner Buchstabe) oder als Langoption (mehrere Buchstaben) angegeben werden.
- Wenn eine Option ein Argument aufweist, ist dieses Argument obligatorisch. Beispiel:

  ```
  ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
  ```

  Dabei ist **ifconfig** der Befehl, "eth0" ist ein Argument und "-i", "-g" und "-s" sind Optionen. In diesem Beispiel weisen alle drei Optionen Argumente auf.
- Eckige Klammern geben an, dass ein Argument oder eine Option optional ist. Dabei sind die eckigen Klammern nicht Teil des Befehls, den Sie eingeben.

Merkmale und Einschränkungen

Die Befehlszeilenschnittstelle weist folgende Merkmale und Einschränkungen auf:

- Mehrere gleichzeitige Befehlszeilenschnittstellensitzungen sind mit verschiedenen Zugriffsmethoden (Telnet oder SSH) zulässig. Es können höchstens zwei Telnet-Befehlszeilensitzungen gleichzeitig aktiv sein.

  Anmerkung: Die Anzahl der Telnet-Sitzung ist konfigurierbar. Gültige Werte sind 0, 1 und 2. Der Wert 0 bedeutet, dass die Telnet-Schnittstelle inaktiviert ist.
- Es ist ein Befehl pro Zeile zulässig (maximal 160 Zeichen, einschließlich Leerzeichen).
- Für lange Befehle gibt es kein Fortsetzungszeichen. Die einzige Editierfunktion ist die Rückschritttaste, mit der Sie das zuvor eingegebene Zeichen löschen können.
- Sie können die Aufwärts- und die Abwärtspfeiltaste verwenden, um durch die letzten acht Befehle zu blättern. Mit dem Befehl **history** können Sie eine Liste der letzten acht Befehle anzeigen, die sie anschließend als Direktaufruf zum Ausführen eines Befehls verwenden können, wie im folgenden Beispiel dargestellt:

  ```
  system> history
   0 ifconfig eth0
   1 readlog
   2 readlog
   3 readlog
   4 history
  ```

```
system> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

- In der Befehlszeilenschnittstelle liegt der Ausgabepuffergrenzwert bei 2 KB. Es gibt keine Pufferung. Die Ausgabe eines einzelnen Befehls darf 2048 Zeichen nicht überschreiten. Dieser Grenzwert gilt nicht im Modus für serielle Umleitung (die Daten werden bei der seriellen Umleitung gepuffert).
- Die Ausgabe eines Befehls erscheint in der Anzeige, nachdem die Ausführung des Befehls beendet ist. Dadurch ist es für Befehle unmöglich, den Echtzeitausführungsstatus zu melden. Beispiel: Im ausführlichen Modus des Befehls **flashing** wird der Vorgang des Blinkens nicht in Echtzeit angezeigt. Er wird erst angezeigt, nachdem die Befehlsausführung beendet ist.
- Der Befehlsausführungsstatus wird durch einfache Textnachrichten angegeben, wie im folgenden Beispiel dargestellt:

  ```
  system> power on
  ok
  system> power state
  Power: On
  State: System power off/State unknown
  system>
  ```

- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Zwischen einer Option und dem zugehörigen Argument muss mindestens ein Leerzeichen stehen. Im Beispiel `ifconfig eth0 -i192.168.70.133` ist die Befehlssyntax falsch. Die richtige Syntax lautet `ifconfig eth0 -i 192.168.70.133`.
- Alle Befehle verfügen über die Optionen `-h`, `-help` und `?`, mit denen Hilfe zur Syntax angezeigt werden kann. Alle der folgenden Beispiele haben dasselbe Ergebnis:

  ```
  system> power -h
  system> power -help
  system> power ?
  ```

- Einige der Befehle, die in den folgenden Abschnitten beschrieben werden, sind möglicherweise nicht verfügbar. Um eine Liste der unterstützten Befehle anzuzeigen, verwenden Sie die Optionen "help" oder "?", wie in den folgenden Beispielen dargestellt:

  ```
  system> help
  system> ?
  ```

Dienstprogrammbefehle

Folgende Dienstprogrammbefehle sind verfügbar:

- exit
- help
- history

Befehl "exit"

Mit dem Befehl **exit** können Sie sich abmelden und die Sitzung der Befehlszeilenschnittstelle beenden.

Befehl "help"

Mit dem Befehl **help** können Sie eine Liste aller Befehle und eine Kurzbeschreibung zu den einzelnen Befehlen anzeigen. Sie können auch **?** an der Eingabeaufforderung eingeben.

Befehl "history"

Mit dem Befehl **history** können Sie eine indexierte Protokollliste der letzten acht Befehle anzeigen, die ausgegeben wurden. Die Indizes können dann als Direktaufrufe (mit davor stehendem !) verwendet werden, um die Befehle aus dieser Protokollliste erneut auszugeben.

Beispiel:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Überwachungsbefehle

Folgende Überwachungsbefehle sind verfügbar:

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

Befehl "clearlog"

Mit dem Befehl **clearlog** können Sie das Ereignisprotokoll des IMM löschen. Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung zu Löschen von Ereignisprotokollen verfügen.

Befehl "fans"

Mit dem Befehl **fans** können Sie die Geschwindigkeit der einzelnen Serverlüfter anzeigen.

Beispiel:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Befehl "readlog"

Mit dem Befehl **readlog** können Sie jeweils fünf IMM-Ereignisprotokolleinträge anzeigen. Die Einträge werden in der Reihenfolge vom aktuellsten bis zum ältesten Eintrag angezeigt.

readlog zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag (bei seiner ersten Ausführung), und dann die nächsten fünf für jeden nachfolgenden Aufruf.

readlog -f setzt den Zähler zurück und zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag.

Syntax:

```
readlog [Optionen]
Option:
-f
```

Beispiel:

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Befehl "syshealth"

Mit dem Befehl **syshealth** können Sie eine Zusammenfassung des Serverzustands anzeigen. Es werden der Stromversorgungsstatus, der Systemstatus, der Zähler für Neustart und der Status der IMM-Software angezeigt.

Beispiel:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

Befehl "temps"

Mit dem Befehl **temps** können Sie alle Temperaturwerte und Temperaturschwellenwerte anzeigen. Dieselben Temperaturwerte werden auch in der Webschnittstelle angezeigt.

Beispiel:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W      T     SS     HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
system>
```

Anmerkungen:

1. Die Ausgabe weist die folgenden Spaltenüberschriften auf:
   WR: Warnungzurücksetzung
   W: Warnung
   T: Temperatur (aktueller Wert)
   SS: Normaler Systemabschluss
   HS: Erzwungener Systemabschluss
2. Alle Temperaturwerte sind in Grad Fahrenheit/Grad Celsius angegeben.

Befehl "volts"

Mit dem Befehl **volts** können Sie alle Spannungswerte und Spannungsschwellenwerte anzeigen. Dieselben Spannungswerte werden auch in der Webschnittstelle angezeigt.

Beispiel:

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Anmerkung: Die Ausgabe weist die folgenden Spaltenüberschriften auf:
HSL: Erzwungener Systemabschluss (Unterspannung)
SSL: Normaler Systemabschluss (Unterspannung)
WL: Warnung (Unterspannung)
WRL: Warnungszurücksetzung (Unterspannung)
V: Spannung (aktueller Wert)
WRH: Warnungszurücksetzung (Überspannung)
WH: Warnung (Überspannung)
SSH: Normaler Systemabschluss (Überspannung)
HSH: Erzwungener Systemabschluss (Überspannung)

Befehl "vpd"

Mit dem Befehl **vpd** können Sie elementare Produktdaten für das System (sys), das IMM, die Server-Firmware (bios) und Dynamic System Analysis Preboot (dsa) anzeigen. Dieselben Informationen werden auch in der Webschnittstelle angezeigt.

Syntax:

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

Beispiel:

```
system> vpd dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
system>
```

Steuerbefehle für Serverstromversorgung und -neustart

Folgende Befehle für Serverstromversorgung und -neustart sind verfügbar:

- power
- reset

Befehl "power"

Mit dem Befehl **power** können Sie die Stromversorgung des Servers steuern. Um die Befehle vom Typ **power** ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen.

power on - Die Serverstromversorgung wird eingeschaltet.

power off - Die Serverstromversorgung wird ausgeschaltet. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

power state - Zeigt den Serverstromversorgungszustand (on oder off) und den aktuellen Zustand des Servers an.

power cycle - Schaltet die Serverstromversorgung zunächst aus und dann wieder ein. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

Befehl "reset"

Mit dem Befehl **reset** können Sie den Server erneut starten. Um diesen Befehl ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server erneut gestartet wird.

Syntax:

```
reset [Option]
Option:
-s
```

Befehl zur seriellen Umleitung

Es gibt nur einen Befehl zur seriellen Umleitung: console.

Befehl "console"

Mit dem Befehl **console** können Sie eine Konsolensitzung mit serieller Umleitung zum designierten seriellen Anschluss des IMM starten.

Syntax:

```
console 1
```

Konfigurationsbefehle

Folgende Konfigurationsbefehle sind verfügbar:

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

Befehl "dhcpinfo"

Mit dem Befehl **dhcpinfo** können Sie die durch den DHCP-Server zugeordnete IP-Konfiguration für eth0 anzeigen, wenn die Schnittstelle automatisch durch einen DHCP-Server konfiguriert wird. Mit dem Befehl **ifconfig** können Sie DHCP aktivieren oder inaktivieren.

Syntax:

```
dhcpinfo eth0
```

Beispiel:

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n     : IMMA-00096B9E003A
-i     : 192.168.70.202
-g     : 192.168.70.29
-s     : 255.255.255.0
-d     : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6    : 0::0
-d6    : *
```

```
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-server	DHCP-Server, der die Konfiguration zugeordnet hat
-n	Zugeordneter Hostname
-i	Zugeordnete IPv4-Adresse
-g	Zugeordnete Gateway-Adresse
-s	Zugeordnete Teilnetzmaske
-d	Zugeordneter Domänenname
-dns1	Primäre IP-Adresse des IPv4-DNS-Servers
-dns2	Sekundäre IPv4-DNS-IP-Adresse
-dns3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i6	IPv6-Adresse
-d6	IPv6-Domänenname
-dns61	Primäre IP-Adresse des IPv6-DNS-Servers
-dns62	Sekundäre IPv6-DNS-IP-Adresse
-dns63	Tertiäre IP-Adresse des IPv6-DNS-Servers

Befehl "dns"

Mit dem Befehl **dns** können Sie die DNS-Konfiguration des IMM anzeigen.

Syntax:

```
dns
```

Anmerkung: Im folgenden Beispiel ist eine IMM-Konfiguration mit aktiviertem DNS dargestellt.

Beispiel:

```
system> dns
-state  : enabled
-i1     : 192.168.70.202
-i2     : 192.168.70.208
-i3     : 192.168.70.212
-i61    : fe80::21a:64ff:fee6:4d5
-i62    : fe80::21a:64ff:fee6:4d6
-i63    : fe80::21a:64ff:fee6:4d7
-ddns   : enabled
-dnsrc  : dhcp
-p     : ipv6

system>
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-state	Zustand des DNS (`enabled` oder `disabled`)
-i1	Primäre IP-Adresse des IPv4-DNS-Servers

Option	Beschreibung
-i2	Sekundäre IPv4-DNS-IP-Adresse
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i61	Primäre IP-Adresse des IPv6-DNS-Servers
-i62	Sekundäre IPv6-DNS-IP-Adresse
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers
-ddns	Zustand des DDNS (`enabled` oder `disabled`)
-dnsrc	Bevorzugter DDNS-Domänenname (`dhcp` oder `manual`)
-p	Bevorzugte DNS-Server (`ipv4` oder `ipv6`)

Befehl "gprofile"

Mit dem Befehl **gprofile** können Sie Gruppenprofile für das IMM anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-clear	Löscht eine Gruppe	Enabled, disabled
-n	Der Name der Gruppe	Zeichenfolge mit bis zu 63 Zeichen für *Gruppenname*. Der *Gruppenname* muss eindeutig sein.
-a	Rollenbasierte Sicherheitsstufe (Berechtigung)	Supervisor, operator, rbs <Rollenliste>: ns | uam | rca | rcrda | rpr | bac | ce | aac Die Rollenlistenwerden in einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, angegeben.
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

```
gprofile [1 - 16] [Optionen]
Optionen:
-clear Status
-n  Gruppenname
-a  Sicherheitsstufe:
    -ns Netzbetrieb und Sicherheit
    -uam Benutzerkontenverwaltung
    -rca Zugriff auf ferne Konsole
    -rcrda Zugriff auf ferne Konsole und fernen Datenträger
    -rpr Zugriff auf Einschalten/Neustart eines fernen Servers
    -bac Allgemeine Adapterkonfiguration
    -ce Fähigkeit zum Löschen von Ereignisprotokollen
    -aac Erweiterte Adapterkonfiguration
-h
```

Befehl "ifconfig"

Mit dem Befehl **ifconfig** können Sie die Ethernet-Schnittstelle konfigurieren. Geben Sie `ifconfig eth0` ein, um die aktuelle Ethernet-Schnittstellenkonfiguration anzuzeigen. Um die Konfiguration der Ethernet-Schnittstelle zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Schnittstellenkonfi-

guration ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-state	Schnittstellenstatus	disabled, enabled
-c	Konfigurationsmethode	dhcp, static, dthens ("dthens" entspricht der Option **Try dhcp server, if it fails use static config** (Nach DHCP-Server suchen. Falls das fehlschlägt, statische Konfiguration verwenden) in der Webschnittstelle)
-i	Statische IP-Adresse	Adresse im gültigen Format
-g	Gateway-Adresse	Adresse im gültigen Format
-s	Teilnetzmaske	Adresse im gültigen Format
-n	Hostname	Zeichenfolge von bis zu 63 Zeichen. Die Zeichenfolge kann Buchstaben, Ziffern, Punkte, Unterstriche und Bindestriche enthalten.
-dn	Domänenname	Domänenname im gültigen Format
-ipv6	IPv6-Status	disabled, enabled
-lla	Lokale Verbindungsadresse **Anmerkung:** Die lokale Verbindungsadresse wird nur angezeigt, wenn IPv6 aktiviert ist.	Die lokale Verbindungsadresse wird vom IMM festgelegt. Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6static	Statischer IPv6-Status	disabled, enabled
-i6	Statische IP-Adresse	Statische IP-Adresse für Ethernet-Kanal 0 im IPv6-Format
-p6	Länge des Adresspräfix	Numerisch zwischen 1 und 128
-g6	Gateway oder Standardroute	IP-Adresse für das Gateway oder die Standardroute für Ethernet-Kanal 0 im IPv6-Format.
-dhcp6	DHCPv6-Status	disabled, enabled
-sa6	Statusunabhängiger IPv6-Status mit automatischer Konfiguration	disabled, enabled
-address_table	Tabelle der automatisch generierten IPv6-Adressen und ihre Präfixlängen **Anmerkung:** Diese Option wird nur dann angezeigt, wenn IPv6 und die statusunabhängige automatische Konfiguration aktiviert sind.	Dieser Wert ist schreibgeschützt und nicht konfigurierbar.

Option	Beschreibung	Werte
-auto	Einstellung für automatische Vereinbarung, die bestimmt, ob die Netzeinstellungen für die Übertragungsgeschwindigkeit und den Duplexmodus konfigurierbar sind.	true, false
-r	Übertragungsgeschwindigkeit	10, 100, auto
-d	Duplexmodus	full, half, auto
-m	MTU	Numerisch zwischen 60 und 1500
-l	LAA	MAC-Adressenformat. Multicastadressen sind nicht zulässig (das erste Byte muss gerade sein).

Syntax:

```
ifconfig eth0 [Optionen]
Optionen:
-state Schnittstellenstatus
-c Konfigurationsmethode
-i statische_IP-Adresse
-g Gatewayadresse
-s Teilnetzmaske
-n Hostname
-r Übertragungsgeschwindigkeit
-d Duplexmodus
-m MTU
-l lokal_verwaltete_MAC-Adresse
```

Beispiel:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

Anmerkung: Die Option **-b** in der Anzeige von "ifconfig" steht für die Herstellerkennung der MAC-Adresse. Die Herstellerkennung der MAC-Adresse ist schreibgeschützt und nicht konfigurierbar.

Befehl "ldap"

Mit dem Befehl **ldap** können Sie die Konfigurationsparameter des LDAP-Protokolls anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-aom	Modus nur für Authentifizierung	Enabled, disabled
-a	Benutzerauthentifizierungsmethode	"Local only", "LDAP only", "Local first then LDAP", "LDAP first then local"
-b	Bindungsmethode	"Bind with Anonymous", "Bind with ClientDN and password" und "Bind with Login Credential"
-c	Definierter Name des Clients	Zeichenfolge mit bis zu 63 Zeichen für *Definierter_Name_des_Clients*
-fn	Gesamtstrukturname	Für Active Directory-Umgebungen, Zeichenfolge mit bis zu 127 Zeichen für *Gesamtstrukturname*
-d	Suchdomäne	Zeichenfolge mit bis zu 31 Zeichen für *Suchdomäne*
-f	Gruppenfilter	Zeichenfolge mit bis zu 63 Zeichen für *Gruppenfilter*
-g	Gruppensuchattribut	Zeichenfolge mit bis zu 63 Zeichen für *Gruppensuchattribut*
-l	Anmeldeberechtigungsattribut	Zeichenfolge mit bis zu 63 Zeichen für *Zeichenfolge*
-p	Clientkennwort	Zeichenfolge mit bis zu 15 Zeichen für *Clientkennwort*
-pc	Clientkennwort bestätigen	Zeichenfolge mit bis zu 15 Zeichen für *Bestätigungskennwort* Befehlssyntax: ldap -p *Clientkennwort* -pc *Bestätigungskennwort* Diese Option ist erforderlich, wenn Sie das Clientkennwort ändern. Sie vergleicht das Argument *Bestätigungskennwort* mit dem Argument *Clientkennwort*. Der Befehl schlägt fehl, wenn die beiden Argumente nicht miteinander übereinstimmen.
-r	Definierter Name des Stammeintrags (DN)	Zeichenfolge mit bis zu 63 Zeichen für *definierter_Rootname*
-rbs	Erweiterte rollenbasierte Sicherheit für Active Directory-Benutzer	Enabled, disabled
s1ip	Hostname/IP-Adresse von Server 1	Zeichenfolge mit bis zu 63 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
s2ip	Hostname/IP-Adresse von Server 2	Zeichenfolge mit bis zu 63 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
s3ip	Hostname/IP-Adresse von Server 3	Zeichenfolge mit bis zu 63 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-s4ip	Hostname/IP-Adresse von Server 4	Zeichenfolge mit bis zu 63 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
s1pn	Portnummer von Server 1	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
s2pn	Portnummer von Server 2	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
s3pn	Portnummer von Server 3	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
s4pn	Portnummer von Server 4	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*

Option	Beschreibung	Werte
-t	Zielname des Servers	Wenn die Option "-rbs" aktiviert ist, gibt dieses Feld einen Zielnamen an, der mithilfe des Snap-ins für die rollenabhängige Sicherheit auf dem Active Directory-Server einem oder mehreren Rollen zugeordnet werden kann.
-u	UID-Suchattribut	Zeichenfolge mit bis zu 23 Zeichen für *Suchattribut*
-v	LDAP-Serveradresse über DNS abrufen	Off, on
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

```
ldap [Optionen]
Optionen:
   -aom enabled|disabled|
   -a loc|ldap|locId|ldloc
   -b anon|client|login
   -c Definierter_Name_des_Clients
   -d Suchdomäne
   -fn Gesamtstrukturname
   -f Gruppenfilter
   -g Gruppensuchattribut
   -l Zeichenfolge
   -p Clientkennwort
   -pc Bestätigungskennwort
   -r definierter_Rootname
   -rbs enabled|disabled
   -s1ip Hostname/IP-Adresse
   -s2ip Hostname/IP-Adresse
   -s3ip Hostname/IP-Adresse
   -s4ip Hostname/IP-Adresse
   -s1pn Portnummer
   -s2pn Portnummer
   -s3pn Portnummer
   -s4pn Portnummer
   -t Name
   -u Suchattribut
   -v off|on
   -h
```

Befehl "ntp"

Mit dem Befehl **ntp** können Sie das Network Time Protocol (NTP) anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Aktiviert oder inaktiviert das Network Time Protocol.	Enabled, disabled
-i	Name oder IP-Adresse des Network Time Protocol-Servers	Der Name des NTP-Servers, der für die Taktgebersynchronisation verwendet werden soll.

Option	Beschreibung	Werte
-f	Die Häufigkeit (in Minuten), mit der der IMM-Taktgeber mit dem Network Time Protocol-Server synchronisiert wird.	3 - 1440 Minuten
-synch	Fordert eine sofortige Synchronisation mit dem Network Time Protocol-Server an	Mit diesem Parameter werden keine Werte verwendet.

Syntax:

```
ntp [Optionen]
Optionen:
-en Zustand
-i  Hostname
-f  Häufigkeit
-synch
```

Beispiel:

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Befehl "passwordcfg"

Mit dem Befehl **passwordcfg** können Sie die Kennwortparameter anzeigen und konfigurieren.

Option	Beschreibung
-legacy	Legt für die Accountsicherheit eine vordefinierte Gruppe von traditionellen Standardwerten fest.
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest.
-exp	Maximale Gültigkeitsdauer des Kennworts (0 - 365 Tage). Der Wert "0" bedeutet, dass das Kennwort nie abläuft.
-cnt	Anzahl der vorherigen Kennwörter, die nicht erneut verwendet werden dürfen (0 - 5).
-nul	Lässt Konten ohne Kennwort zu (yes | no)
-h	Zeigt die Befehlssyntax und die Optionen an

Syntax:

```
passwordcfg [Optionen]
Optionen: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Beispiel:

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

Befehl "portcfg"

Mit dem Befehl **portcfg** können Sie den seriellen Anschluss konfigurieren. Um die Konfiguration des seriellen Anschlusses zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration des seriellen Anschlusses ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

Die Parameter werden in der Hardware festgelegt und können nicht geändert werden:
- 8 Datenbit
- Keine Parität
- 1 Stoppbit

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-b	Baudrate	9600, 19200, 38400, 57600, 115200, 230400
-climode	CLI-Modus	none, cliems, cliuser • none: Die Befehlszeilenschnittstelle (CLI) ist inaktiviert • cliems: Die Befehlszeilenschnittstelle ist mit EMS-kompatiblen Tastenfolgen aktiviert • cliuser: Die Befehlszeilenschnittstelle ist mit benutzerdefinierten Tastenfolgen aktiviert

Syntax:

```
portcfg [Optionen]
portcfg [Optionen]
Optionen:
-b Baudrate
-climode CLI-Modus
-cliauth CLI-Authentifizierung
```

Beispiel:

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

Befehl "portcontrol"

Verwenden Sie den Befehl **portcontrol**, um den Portstatus des IMM-Service zu konfigurieren. Um den Portstatus zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um den Portsteuerungsstatus ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-ipmi	IPMI-Port	on, off

Syntax:

```
portcontrol [Optionen]
Optionen:
-ipmi Status
```

Beispiel:

```
system> portcontrol
-ipmi: on
```

Befehl "srcfg"

Mit dem Befehl **srcfg** können Sie die serielle Umleitung konfigurieren. Geben Sie `srcfg` ein, um die aktuelle Konfiguration anzuzeigen. Um die Konfiguration der seriellen Umleitung zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration der seriellen Umleitung ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

In der folgenden Tabelle sind die Argumente für die Option `-exitcliseq` aufgelistet.

Option	Beschreibung	Werte
-exitcliseq	Tastenfolge zum Verlassen der Befehlszeilenschnittstelle (CLI)	Benutzerdefinierte Tastenfolge zum Verlassen der Befehlszeilenschnittstelle. Ausführliche Informationen dazu finden Sie bei den Werten für die Option "-entercliseq" in dieser Tabelle.

Syntax:

```
srcfg [Optionen]
Optionen:
-exitcliseq exitcli_keyseq
```

Beispiel:

```
system> srcfg
-exitcliseq ^[Q
system>
```

Befehl "ssl"

Mit dem Befehl **ssl** können Sie die SSL-Parameter (Secure Sockets Layer) anzeigen und konfigurieren.

Anmerkung: Bevor Sie einen SSL-Client aktivieren können, muss ein Clientzertifikat installiert werden.

Option	Beschreibung
-ce	Aktiviert oder inaktiviert einen SSL-Client
-se	Aktiviert oder inaktiviert einen SSL-Server
-h	Listet die Befehlssyntax und die Optionen auf

Syntax:

```
ssl [Optionen]
Optionen:
-ce on | off
-se on | off
-h
```

Parameter: Die folgenden Parameter erscheinen in der Optionsstatusanzeige für den Befehl **ssl** und werden nur über die Befehlszeilenschnittstelle ausgegeben:

Server secure transport enable (Sichere Serverübertragung aktivieren)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden.

Server Web/CMD key status (Server-Web/CMD-Schlüsselstatus)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status (CSR-Schlüssel für SSL-Server)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL Client LDAP key status (LDAP-Schlüssel für SSL-Client)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL Client CSR key status (CSR-Schlüssel für SSL-Client)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

Befehl "timeouts"

Mit dem Befehl **timeouts** können Sie die Zeitlimitwerte anzeigen oder ändern. Um die Zeitlimitwerte anzuzeigen, geben Sie `timeouts` ein. Um die Zeitlimitwerte zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um Zeitlimitwerte ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Configuration" (Adapterkonfiguration) verfügen.

In der folgenden Tabelle sind die Argumente für die Zeitlimitwerte aufgelistet. Diese Werte entsprechen den abgestuften Pulldownoptionsskalen für Serverzeitlimits in der Webschnittstelle.

Option	Zeitlimit	Einheiten	Werte
-o	Zeitlimit für das Betriebssystem	Minuten	disabled, 2.5, 3, 3.5, 4
-l	Zeitlimit für das Ladeprogramm	Minuten	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Syntax:

```
timeouts [Optionen]
Optionen:
-o Option_für_Betriebssystem-Watchdog
-l Option_für_Ladeprogramm-Watchdog
```

Beispiel:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

Befehl "usbeth"

Mit dem Befehl **usbeth** können Sie die Inbandschnittstelle "LAN over USB" aktivieren oder inaktivieren. Weitere Informationen zum Aktivieren und Inaktivieren dieser Schnittstelle finden Sie unter „USB-Inband-Schnittstelle inaktivieren” auf Seite 26.

Syntax:

```
usbeth [Optionen]
Optionen:
-en <enabled|disabled>
```

Beispiel:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Befehl "users"

Mit dem Befehl **users** können Sie auf alle Benutzerkonten und auf die zugehörigen Berechtigungsstufen zugreifen, neue Benutzerkonten erstellen und bereits vorhandene Konten ändern.

Beachten Sie die folgenden Richtlinien zum Befehl **users**:

- Benutzernummern werden von 1 bis 12 einschließlich angegeben.
- Benutzernamen müssen weniger als 16 Zeichen enthalten und dürfen nur aus Zahlen, Buchstaben, Punkten und Unterstreichungszeichen bestehen.
- Kennwörter müssen mindestens 5 Zeichen und dürfen höchstens 16 Zeichen lang sein. Sie müssen mindestens ein alphabetisches und mindestens nichtalphabetisches Zeichen enthalten.
- Als Berechtigungsstufe kann eine der folgenden Stufen angegeben werden:
  - super (Supervisor)
  - ro (Lesezugriff)
  - Eine beliebige Kombination aus den folgenden Werten, getrennt durch |:
    - am (Benutzerkontenverwaltungszugriff)
    - rca (Zugriff auf ferne Konsole)
    - rcvma (Zugriff auf ferne Konsole und virtuelle Datenträger)
    - pr (Zugriff auf Einschalten/Neustart eines fernen Servers)
    - cel (Berechtigung zum Löschen von Ereignisprotokollen)
    - bc (Adapterkonfiguration [einfach])
    - nsc (Adapterkonfiguration [Netz und Sicherheit])
    - ac (Adapterkonfiguration [erweitert])

Syntax:

```
users [Optionen]
Optionen:
-Benutzernummer
-n Benutzername
-p Kennwort
-a Berechtigungsstufe
```

Beispiel:

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration

4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
```

```
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM-Steuerbefehle

Folgende IMM-Steuerbefehle sind verfügbar:

- clearcfg
- clock
- identify
- resetsp
- update

Befehl "clearcfg"

Verwenden Sie den Befehl **clearcfg**, um die IMM-Konfiguration auf die werkseitigen Voreinstellungen zurückzusetzen. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können. Nachdem die Konfiguration des IMM gelöscht ist, wird das IMM erneut gestartet.

Befehl "clock"

Mit dem Befehl **clock** können Sie das aktuelle Datum und die aktuelle Uhrzeit entsprechend der IMM-Uhr und der GMT-Abweichung anzeigen. Sie können das Datum, die Uhrzeit, die GMT-Abweichung und die Sommerzeiteinstellungen festlegen.

Beachten Sie Folgendes:

- Für eine GMT-Abweichung von +2 oder +10 sind besondere Einstellungen für die Sommerzeit erforderlich.
- Für +2 gibt es folgende Optionen für die Sommerzeit: off, ee (Osteuropa), gtb (Großbritannien), egt (Ägypten), fle (Finnland).
- Für +10 gibt es folgende Sommerzeiteinstellungen: off, ea (Ostaustralien), tas (Tasmanien), vlad (Wladiwostok).
- Das Jahr muss von 2000 bis einschließlich 2089 angegeben werden.
- Monat, Datum, Stunden, Minuten und Sekunden können als Einzelzifferwerte angegeben werden (z. B. 9:50:25 anstatt 09:50:25).
- Die GMT-Abweisung kann im Format +2:00, +2 oder 2 (für positive Abweichungen) und im Format -5:00 oder -5 (für negative Abweichungen) angegeben werden.

Syntax:

```
clock [Optionen]
Optionen:
-d mm/tt/jjjj
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Beispiel:

```
system> clock
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

Befehl "identify"

Mit dem Befehl **identify** können Sie die Gehäusekennzeichnungsanzeige einschalten, ausschalten oder blinken lassen. Die Option -d kann zusammen mit -s verwendet werden, um die Anzeige nur für eine bestimmte Anzahl an Sekunden einzuschalten, die mit dem Parameter -d angegeben werden. Nachdem die Anzahl an Sekunden verstrichen ist, wird die Anzeige ausgeschaltet.

Syntax:

```
identify [Optionen]
Optionen:
-s on/off/blink
-d Sekunden
```

Beispiel:

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Befehl "resetsp"

Mit dem Befehl **resetsp** können Sie das IMM erneut starten. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

Befehl "update"

Mit dem Befehl **update** können Sie die Firmware auf dem IMM oder das IMM aktualisieren. Um diesen Befehl verwenden zu können, müssen Sie mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen. Die Firmwaredatei (angegeben durch *Dateiname*) wird zuerst vom TFTP-Server (angegeben durch seine IP-Adresse) zum IMM übertragen und dann über Flashing aktualisiert. Die Option **-v** gibt den ausführlichen Modus an.

Anmerkung: Stellen Sie sicher, dass der TFTP-Server auf dem Server, von dem die Datei heruntergeladen wird, ausgeführt wird.

Option	Beschreibung
-i	IP-Adresse des TFTP-Servers
-l	Dateiname (für Flashing)
-v	Ausführlicher Modus

Syntax:

```
update -i IP-Adresse_des_TFTP-Servers -l Dateiname
```

Beispiel: Im ausführlichen Modus wird der Flashingfortschritt in Echtzeit als Prozentsatz der Fertigstellung angezeigt.

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

Wenn das Flashing nicht im ausführlichen Modus ausgeführt wird, wird der Fortschritt in aufeinanderfolgenden #-Zeichen dargestellt.

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ##################################################
Flashing image: ##################################################
Flash operation completed.
```

Service Advisor-Befehle

Folgende Service Advisor-Befehle sind verfügbar:

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

Befehl "autoftp"

Mit dem Befehl **autoftp** können Sie die FTP-/TFTP-Servereinstellungen für den Service Advisor anzeigen und konfigurieren.

Anmerkung: Sie müssen zuerst die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie diesen Befehl verwenden können.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-m	Automatisierter Problemmeldungs-modus	*ftp, tftp, disabled*
-i	IP-Adresse oder Hostname des FTP-/TFTP-Servers für die automatisierte Problemmeldung	IP-Adresse oder Hostname
-p	FTP/TFTP-Übertragungsport	Numerischer Wert von 1 bis 65535 für *Portnummer*
-u	Durch Anführungs-zeichen begrenzter FTP-Benutzername für die Problemmeldung	Zeichenfolge mit bis zu 63 Zeichen für *Benutzername*
-pw	Durch Anführungs-zeichen begrenztes FTP-Kennwort für die Problemmeldung	Zeichenfolge mit bis zu 63 Zeichen für *Kennwort*
Anmerkung: Für den Wert *ftp* müssen alle Optionen (die Felder -i, -p, -u und -pw) festgelegt werden. Für den Wert *tftp* sind nur die Optionen -i und -p erforderlich.		

Syntax:

```
autoftp [Optionen]
Optionen:
-m ftp|tftp|disable
-i Hostname|IP-Adresse
-p Portnummer
-u Benutzername
-pw Kennwort
```

Befehl "chconfig"

Mit dem Befehl **chconfig** können Sie die Service Advisor-Einstellungen für das IMM anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-li	Nutzungsbedingungen von Service Advisor anzeigen oder akzeptieren. Sie müssen zuerst über diese Option die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie weitere Optionen festlegen können.	view, accept
-sa	IBM Support-Status von Service Advisor	enabled, disabled
-sc	Landescode für das IBM Service Support Center	ISO-Landescode aus zwei Zeichen
-ca	Durch Anführungszeichen begrenzte Adresse des Maschinenstandorts	Zeichenfolge mit bis zu 30 Zeichen für *Adresse*
-cci	Durch Anführungszeichen begrenzter Ort des Maschinenstandorts	Zeichenfolge mit bis zu 30 Zeichen für *Ort*

Option	Beschreibung	Werte
-ce	E-Mail-Adresse des Ansprechpartners im Format *userid@hostname*	Zeichenfolge mit bis zu 30 Zeichen für *E-Mail-Adresse*
-cn	Durch Anführungszeichen begrenzter Name des Ansprechpartners	Zeichenfolge mit bis zu 30 Zeichen für *Ansprechpartner*
-co	Durch Anführungszeichen begrenzter Name der Organisation/des Unternehmens des Ansprechpartners	Zeichenfolge mit bis zu 30 Zeichen für *Unternehmensname*
-cph	Durch Anführungszeichen begrenzte Telefonnummer des Ansprechpartners	Zeichenfolge mit 5 bis 30 Zeichen für *Telefonnummer*
-cs	Bundesland des Maschinenstandorts	Zeichenfolge mit 2 bis 3 Zeichen für *Bundesland*
-cz	Durch Anführungszeichen begrenzte Postleitzahl des Maschinenstandorts	Zeichenfolge mit bis zu 9 Zeichen für *Postleitzahl*
-loc	Vollständig qualifizierter Hostname oder IP-Adresse für HTTP-Proxy	Zeichenfolge mit bis zu 63 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-po	Port des HTTP-Proxy	Eine numerische Portnummer zwischen 1 und 65535 für *Portnummer*
-ps	Status des HTTP-Proxy	enabled, disabled
-pw	Durch Anführungszeichen begrenztes Kennwort des HTTP-Proxy	Zeichenfolge mit bis zu 15 Zeichen für *Kennwort*
-u	Durch Anführungszeichen begrenzter Benutzername des HTTP-Proxy	Zeichenfolge mit bis zu 30 Zeichen für *Benutzername*

1. Sie müssen zuerst über die Option -li die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie weitere Optionen festlegen können.
2. Alle Felder mit Kontaktinformationen und alle Felder für IBM Service Support Center sind erforderlich, bevor IBM Support für Service Advisor aktiviert werden kann. Wenn ein Proxy erforderlich ist, müssen die Felder für den HTTP-Proxy angegeben werden.

Syntax:

```
chconfig [Optionen]
Optionen:
-li view|accept
-sa Status des Service Advisor
-sc Landescode
-ca Adresse
-cci Ort
-ce E-Mail-Adresse
-cn Name_des_Ansprechpartners
-co Unternehmensname
-cph Telefonnummer
-cs Bundesland
-cz Postleitzahl
-loc Hostname/IP-Adresse
-po Portnummer
-ps Status
-pw Kennwort
-u Benutzername
```

Befehl "chlog"

Mit dem Befehl **chlog** können Sie die letzten fünf Call-Home-Ereignisse anzeigen, die vom System oder vom Benutzer generiert wurden. Der letzte Call-Home-Eintrag wird in der Liste als erstes aufgeführt.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Anmerkung: Sie müssen zuerst die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie diesen Befehl verwenden können.

Option	Beschreibung	Werte
-event_index	Einen Call-Home-Eintrag mithilfe des Index des Aktivitätenprotokolls angeben	Numerisch zwischen 1 und 5
-ack	Bestätigt/Unbestätigt, ein Call-Home-Ereignis wurde korrigiert	yes, no
-s	Nur das Ergebnis von IBM Support anzeigen	
-f	Nur das Ergebnis des FTP-/TFTP-Servers anzeigen	

Syntax:

```
chlog [Optionen]
Optionen:
-event_index
-ack yes|no
-s
-f
```

Befehl "chmanual"

Mit dem Befehl **chmanual** können Sie ein manuelles Call-Home-Ereignis oder ein Call-Home-Test-Ereignis generieren.

Anmerkung: Sie müssen zuerst die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie diesen Befehl verwenden können.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-test	Call-Home-Test-Ereignis generieren	
-desc	Durch Anführungszeichen begrenzte Problembeschreibung	Zeichenfolge mit bis zu 100 Zeichen für *Beschreibung*

Syntax:

```
chmanual [Optionen]
Optionen:
-test
-desc Beschreibung
```

Befehl "events"

Mithilfe des Befehls **events** können Sie Ausschlussereignisse anzeigen und bearbeiten.

Anmerkung: Sie müssen zuerst die Nutzungsbedingungen von Service Advisor akzeptieren, bevor Sie diesen Befehl verwenden können.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-che	Ausschlussereignisse anzeigen und bearbeiten	
-add	Ein Call-Home-Ereignis zur Call-Home-Ausschlussliste hinzufügen	*Ereignis-ID* im Format `0xhhhhhhhhhhhhhhhh`
-rm	Ein Call-Home-Ereignis aus der Call-Home-Ausschlussliste entfernen	*Ereignis-ID*|*all* im Format `0xhhhhhhhhhhhhhhhh` oder "all"

Syntax:

```
events [Optionen]
Optionen: -che {-add}|{-rm}
-add Ereignis-ID
-rm Ereignis-ID|all
```

Befehl "sdemail"

Mit dem Befehl **sdemail** können Sie E-Mail-Serviceinformationen für die angegebenen Empfänger konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-subj	Durch Anführungszeichen begrenzter E-Mail-Betreff	Zeichenfolge mit bis zu 119 Zeichen für *E-Mail-Betreff*
-to	E-Mail-Adresse des Empfängers. Diese Option kann aus mehreren, durch Kommata voneinander getrennten Adressen bestehen.	Zeichenfolge mit bis zu 119 Zeichen für *E-Mail-Adressen*

Syntax:

```
sdemail [Optionen]
Optionen:
-subj E-Mail-Betreff
-to E-Mail-Adressen
```

Anhang A. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Service oder technische Unterstützung benötigen oder einfach nur Informationen zu IBM-Produkten erhalten möchten, finden Sie bei IBM eine Vielzahl von hilfreichen Quellen.

Verwenden Sie diese Informationen, um zusätzliche Informationen zu IBM und IBM Produkten zu erhalten, um herauszufinden, was Sie bei Problemen mit Ihrem IBM System oder Ihrer Zusatzeinrichtung tun können und an wen Sie sich wenden können, wenn Sie Service benötigen.

Bevor Sie sich an den Kundendienst wenden

Stellen Sie sicher, bevor Sie sich an den Kundendienst wenden, dass Sie die folgenden Schritte durchgeführt haben, um zu versuchen, das Problem selbst zu beheben.

Wenn Sie denken, dass Sie den IBM Herstellerservice für Ihr IBM Produkt in Anspruch nehmen müssen, können die IBM Kundendiensttechniker Sie besser unterstützen, wenn Sie sich vor Ihrem Anruf beim Kundendienst vorbereiten.

- Überprüfen Sie alle Kabel und vergewissern Sie sich, dass diese angeschlossen sind.
- Prüfen Sie an den Netzschaltern, ob das System und die Zusatzeinrichtungen eingeschaltet sind.
- Überprüfen Sie, ob aktualisierte Software, Firmware und Einheitentreiber für das Betriebssystem Ihres IBM Produkts vorhanden sind. In den Bedingungen des freiwilligen IBM Herstellerservices steht, dass Sie als Eigentümer des Produkts dafür verantwortlich sind, die Software und Firmware für das Produkt zu warten und zu aktualisieren (es sei denn, dies ist durch einen zusätzlichen Wartungsvertrag abgedeckt). Der IBM Kundendiensttechniker wird Sie dazu auffordern, ein Upgrade für Ihre Software und Firmware durchzuführen, wenn in einem Software-Upgrade eine dokumentierte Lösung für das Problem vorhanden ist.
- Wenn Sie neue Hardware oder Software in Ihrer Umgebung installiert haben, überprüfen Sie unter http://www.ibm.com/systems/info/x86servers/serverproven/compat/us, ob die Hardware und Software von Ihrem IBM Produkt unterstützt werden.
- Rufen Sie die folgende Seite auf http://www.ibm.com/supportportal, um nach Informationen zu suchen, die Ihnen bei der Fehlerbehebung helfen können.
- Stellen Sie für den IBM Support folgende Informationen zusammen. Mithilfe dieser Daten findet der IBM Support schnell eine Lösung für Ihr Problem und kann sicherstellen, dass Sie genau die Servicestufe erhalten, die Sie vertraglich vereinbart haben.
  - Hardware- und Softwarewartungsvertragsnummern, falls vorhanden
  - Maschinentypnummer (vierstellige IBM Maschinenkennung)
  - Modellnummer
  - Seriennummer
  - Aktuelle UEFI- und Firmwareversionen des Systems
  - Andere relevante Informationen wie z. B. Fehlernachrichten und -protokolle

- Rufen Sie die folgende Seite auf http://www.ibm.com/support/entry/portal/Open_service_request, um eine ESR (Electronic Service Request - elektronische Serviceanforderung) zu senden. Wenn Sie eine ESR senden, beginnt der Lösungsfindungsprozess für Ihr Problem, da die relevanten Informationen dem IBM Support schnell und effizient zur Verfügung gestellt werden. IBM Kundendiensttechniker können mit der Fehlerbehebung beginnen, sobald Sie eine ESR ausgefüllt und übergeben haben.

Viele Fehler können ohne Hilfe von außen anhand der IBM Hinweise zur Fehlerbehebung in der Onlinehilfefunktion oder in der Dokumentation, die im Lieferumfang Ihres IBM Produkts enthalten ist, behoben werden. In der Begleitdokumentation der IBM Systeme sind auch die Diagnosetests beschrieben, die Sie ausführen können. Im Lieferumfang der meisten Systeme, Betriebssysteme und Programme sind eine Dokumentation zu Fehlerbehebungsprozeduren sowie Erläuterungen zu Fehlernachrichten und Fehlercodes enthalten. Wenn Sie einen Softwarefehler vermuten, finden Sie weitere Informationen dazu in der Dokumentation zum Betriebssystem oder zum Programm.

Dokumentation verwenden

Informationen zu Ihrem IBM System und, falls vorhanden, zu vorinstallierter Software sowie zu Zusatzeinrichtungen finden Sie in der mit dem Produkt gelieferten Dokumentation. Zu dieser Dokumentation können gedruckte Dokumente, Onlinedokumente, Readme-Dateien und Hilfedateien gehören.

Anweisungen zur Verwendung der Diagnoseprogramme finden Sie in den Fehlerbehebungsinformationen in der Systemdokumentation. Über die Fehlerbehebungsinformationen oder die Diagnoseprogramme erfahren Sie möglicherweise, dass Sie zusätzliche oder aktuelle Einheitentreiber oder andere Software benötigen. IBM verwaltet Seiten im World Wide Web, über die Sie nach den neuesten technischen Informationen suchen und Einheitentreiber und Aktualisierungen herunterladen können. Für den Zugriff auf diese Seiten rufen Sie die Website http://www.ibm.com/supportportal auf.

Hilfe und Informationen über das World Wide Web anfordern

Aktuelle Informationen zu IBM Produkten und zur Unterstützung sind im World Wide Web verfügbar.

Im World Wide Web finden Sie aktuelle Informationen zu IBM Systemen, Zusatzeinrichtungen, Services und Unterstützung unter http://www.ibm.com/supportportal. Informationen zu IBM System x finden Sie unter http://www.ibm.com/systems/x. Informationen zu IBM BladeCenter finden Sie unter http://www.ibm.com/systems/bladecenter. Informationen zu IBM IntelliStation finden Sie unter http://www.ibm.com/systems/intellistation.

Vorgehensweise zum Senden von DSA-Daten an IBM

Senden Sie Ihre Diagnosedaten über das IBM Enhanced Customer Data Repository (ECuRep) an IBM.

Lesen Sie vor dem Senden von Diagnosedaten an IBM die Nutzungsbedingungen unter http://www.ibm.com/de/support/ecurep/terms.html.

Sie können eine der folgenden Methoden zum Senden von Diagnosedaten an IBM verwenden:

- **Standardupload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standardupload mit der Seriennummer des Systems:** http://www.ecurep.ibm.com/app/upload_hw
- **Sicherer Upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Sicherer Upload mit der Seriennummer des Systems:** https://www.ecurep.ibm.com/app/upload_hw

Personalisierte Unterstützungswebseite erstellen

Durch die gezielte Angabe von IBM Produkten, an denen Sie interessiert sind, können Sie eine personalisierte Unterstützungswebseite erstellen.

Wenn Sie eine personalisierte Unterstützungswebseite erstellen möchten, rufen Sie folgende Adresse auf http://www.ibm.com/support/mynotifications. Über diese personalisierte Seite können Sie wöchentliche E-Mail-Benachrichtigungen zu neuen technischen Dokumenten abonnieren, nach Informationen und Downloads suchen und auf verschiedene Verwaltungsservices zugreifen.

Software-Service und -unterstützung

Über die IBM Support Line erhalten Sie gegen eine Gebühr telefonische Unterstützung bei Problemen mit der Nutzung, der Konfiguration und der Software von IBM Produkten.

Informationen dazu, welche Produkte von der Support Line in Ihrem Land oder in Ihrer Region unterstützt werden, finden Sie unter http://www.ibm.com/services/supline/products.

Für weitere Informationen zur Support Line und zu anderen IBM Services rufen Sie http://www.ibm.com/services auf. Telefonnummern für Unterstützung finden Sie, wenn Sie http://www.ibm.com/planetwide aufrufen. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

Hardware-Service und -unterstützung

Hardware-Service können Sie über den IBM Reseller oder den IBM Kundendienst erhalten.

Um nach einem Reseller zu suchen, der durch IBM zur Bereitstellung von Herstellerservice autorisiert wurde, rufen Sie http://www.ibm.com/partnerworld auf und klicken Sie auf **Business Partner Locator**. Telefonnummern für technische Unterstützung von IBM finden Sie unter http://www.ibm.com/planetwide. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

In den USA und in Kanada ist Hardware-Service und -unterstützung jederzeit rund um die Uhr erhältlich. In Großbritannien sind diese Serviceleistungen von Montag bis Freitag von 9 bis 18 Uhr verfügbar.

IBM Produktservice in Taiwan

Wenden Sie sich mithilfe dieser Informationen an den IBM Produktservice in Taiwan.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

Kontaktinformationen für den IBM Produktservice in Taiwan:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telefon: 0800-016-888

Anhang B. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Die auf diesen Websites verfügbaren Informationen beziehen sich nicht auf die für dieses IBM Produkt bereitgestellten Informationen. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Marken

IBM, das IBM Logo und ibm.com sind eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe und PostScript sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Intel, Intel Xeon, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Wichtige Hinweise

Die Prozessorgeschwindigkeit bezieht sich auf die interne Taktgeschwindigkeit des Mikroprozessors. Das Leistungsverhalten der Anwendung ist außerdem von anderen Faktoren abhängig.

Die Geschwindigkeit von CD- oder DVD-Laufwerken wird als die variable Lesegeschwindigkeit angegeben. Die tatsächlichen Geschwindigkeiten können davon abweichen und liegen oft unter diesem Höchstwert.

Bei Angaben in Bezug auf Hauptspeicher, realen/virtuellen Speicher oder Kanalvolumen steht die Abkürzung KB für 1.024 Bytes, MB für 1.048.576 Bytes und GB für 1.073.741.824 Bytes.

Bei Angaben zur Kapazität von Festplattenlaufwerken oder zu Übertragungsgeschwindigkeiten steht die Abkürzung MB für 1.000.000 Bytes und GB für 1.000.000.000 Bytes. Die gesamte für den Benutzer verfügbare Speicherkapazität kann je nach Betriebsumgebung variieren.

Die maximale Kapazität von internen Festplattenlaufwerken geht vom Austausch aller Standardfestplattenlaufwerke und der Belegung aller Festplattenlaufwerkpositionen mit den größten derzeit unterstützten Laufwerken aus, die IBM zur Verfügung stellt.

Zum Erreichen der maximalen Speicherkapazität muss der Standardspeicher möglicherweise durch ein optionales Speichermodul ersetzt werden.

Jede Halbleiterspeicherzelle verfügt über eine intrinsische, endliche Zahl von Schreibzyklen, welche die Zelle ausführen kann. Daher hat eine Halbleitereinheit eine maximale Anzahl von Schreibzyklen, die darauf ausgeführt werden können. Diese wird in TBW (total bytes written - Gesamtzahl der geschriebenen Bytes) angegeben. Hat eine Einheit dieses Limit überschritten, antwortet sie möglicherweise nicht mehr auf vom System generierte Befehle oder kann nicht mehr beschrieben werden.

IBM ist nicht für den Austausch einer Einheit verantwortlich, die ihre maximale Anzahl garantierter Programmierungs-/Löschzyklen überschritten hat, welche in den offiziellen, veröffentlichten Spezifikationen dieser Einheit dokumentiert ist.

IBM enthält sich jeder Äußerung in Bezug auf ServerProven-Produkte und -Services anderer Unternehmen und übernimmt für diese keinerlei Gewährleistung. Dies gilt unter anderem für die Gewährleistung der Gebrauchstauglichkeit und der Eignung für einen bestimmten Zweck. Für den Vertrieb dieser Produkte sowie entsprechende Gewährleistungen sind ausschließlich die entsprechenden Fremdanbieter zuständig.

IBM übernimmt keine Verantwortung oder Gewährleistungen bezüglich der Produkte anderer Hersteller. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch IBM.

Manche Software unterscheidet sich möglicherweise von der im Einzelhandel erhältlichen Version (falls verfügbar) und enthält möglicherweise keine Benutzerhandbücher bzw. nicht alle Programmfunktionen.

Verunreinigung durch Staubpartikel

Achtung: Staubpartikel in der Luft (beispielsweise Metallsplitter oder andere Teilchen) und reaktionsfreudige Gase, die alleine oder in Kombination mit anderen Umgebungsfaktoren, wie Luftfeuchtigkeit oder Temperatur, auftreten, können für die in diesem Dokument beschriebene Einheit ein Risiko darstellen.

Zu den Risiken, die aufgrund einer vermehrten Staubbelastung oder einer erhöhten Konzentration gefährlicher Gase bestehen, zählen Beschädigungen, die zu einer Störung oder sogar zum Totalausfall der Einheit führen. Durch die in dieser Spezifikation festgelegten Grenzwerte für Staubpartikel und Gase sollen solche Beschädigungen vermieden werden. Diese Grenzwerte sind nicht als unveränderliche Grenzwerte zu betrachten oder zu verwenden, da viele andere Faktoren, wie z. B. die Temperatur oder der Feuchtigkeitsgehalt der Luft, die Auswirkungen von Staubpartikeln oder korrosionsfördernden Stoffen in der Umgebung sowie die Verbreitung gasförmiger Verunreinigungen beeinflussen können. Sollte ein bestimmter Grenzwert in diesem Dokument fehlen, müssen Sie versuchen, die Verunreinigung durch Staubpartikel und Gase so gering zu halten, dass die Gesundheit und die Sicherheit der beteiligten Personen dadurch nicht gefährdet sind. Wenn IBM feststellt, dass die Einheit aufgrund einer erhöhten Konzentration von Staubpartikeln oder Gasen in Ihrer Umgebung beschädigt wurde, kann IBM die Reparatur oder den Austausch von Einheiten oder Teilen unter der Bedingung durchführen, dass geeignete Maßnahmen zur Minimierung solcher Verunreinigungen in der Umgebung der Einheit ergriffen werden. Die Durchführung dieser Maßnahmen obliegt dem Kunden.

Tabelle 21. Grenzwerte für Staubpartikel und Gase

Verunreinigung	Grenzwerte
Staubpartikel	• Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52.2[1] gefiltert werden. • Die Luft in einem Rechenzentrum muss mit einem Wirkungsgrad von mindestens 99,97 % mit HEPA-Filtern (HEPA - High-Efficiency Particulate Air) gefiltert werden, die gemäß MIL-STD-282 getestet wurden. • Die relative hygroskopische Feuchtigkeit muss bei Verunreinigung durch Staubpartikel mehr als 60 % betragen[2]. • Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.
Gase	• Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985[3] • Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Die relative hygroskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die relative Feuchtigkeit, bei der der Staub genug Wasser absorbiert, um nass zu werden und Ionen leiten zu können.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Dokumentationsformat

Die Veröffentlichungen für dieses Produkt liegen im PDF-Format vor und entsprechen den handelsüblichen Zugriffsstandards. Falls beim Verwenden der PDF-Dateien Probleme auftreten und Sie ein webbasiertes Format oder ein barrierefreies PDF-Dokument für eine Veröffentlichung anfordern möchten, wenden Sie sich schriftlich an folgende Adresse:

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

Geben Sie in der Anforderung die Teilenummer und den Titel der Veröffentlichung an.

Werden an IBM Informationen eingesandt, gewährt der Einsender IBM ein nicht ausschließliches Recht zur beliebigen Verwendung oder Verteilung dieser Informationen, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Vorschriften zur Telekommunikation

Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Wenden Sie sich bei Fragen an einen IBM Ansprechpartner oder IBM Reseller.

Hinweise zur elektromagnetischen Verträglichkeit

Wenn Sie einen Bildschirm an das Gerät anschließen, müssen Sie das dazugehörige Bildschirmkabel und jede Störschutzeinheit, die im Lieferumfang des Bildschirms enthalten ist, verwenden.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
E-Mail: lugi@de.ibm.com

Deutschland, Hinweis zur Klasse A

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:

International Business Machines Corp. New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Deutschland
Telefon: +49 7032 15 2941
E-Mail: lugi@de.ibm.com

Generelle Informationen:

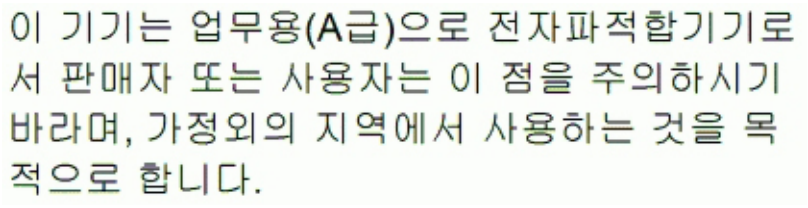
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement



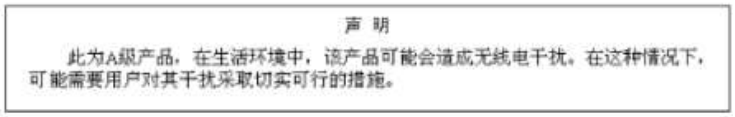
This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

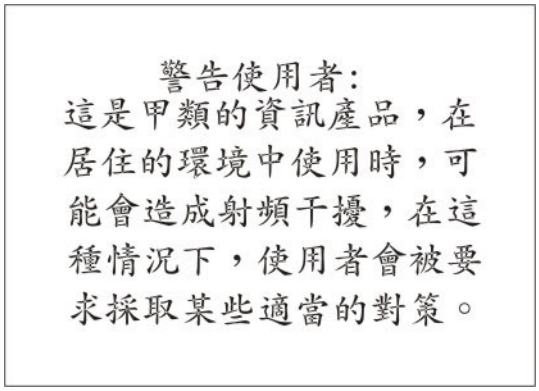
ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明



Taiwan Class A compliance statement



Index

T

U

V

W

Z

Teilenummer: 00FH266

(1P) P/N: 00FH266